

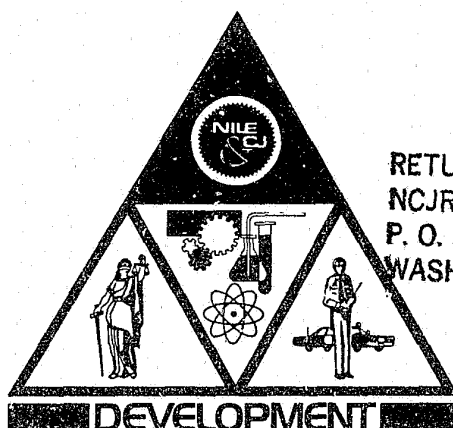
EQUIPMENT SYSTEMS IMPROVEMENT PROGRAM

BURGLARY ALARM SYSTEM Development Program

FINAL REPORT

Law Enforcement Development Group

March 1977



LOAN DOCUMENT

RETURN TO:
NCJRS

P. O. BOX 24036 S. W. POST OFFICE
WASHINGTON, D.C. 20024

Prepared for

National Institute of Law Enforcement and Criminal Justice
LAW ENFORCEMENT ASSISTANCE ADMINISTRATION
U.S. DEPARTMENT OF JUSTICE

The Aerospace Corporation



42351
C-2

EQUIPMENT SYSTEMS IMPROVEMENT PROGRAM
FINAL REPORT
BURGLARY ALARM SYSTEM DEVELOPMENT PROGRAM

Law Enforcement Development Group
THE AEROSPACE CORPORATION
El Segundo, California

March 1977

NC 13

JUL 1 1977

ACQUISITIONS

Prepared for
National Institute of Law Enforcement
and Criminal Justice
LAW ENFORCEMENT ASSISTANCE ADMINISTRATION
U.S. DEPARTMENT OF JUSTICE

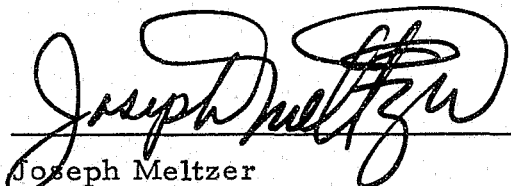
Contract No. J-LEAA-025-73

This project was supported by Contract Number J-LEAA-025-73 awarded by the National Institute of Law Enforcement and Criminal Justice, Law Enforcement Assistance Administration, U.S. Department of Justice, under the Omnibus Crime Control and Safe Streets Act of 1968, as amended. Points of view or opinions stated in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Report No.
ATR-77(7617-04)-1

EQUIPMENT SYSTEMS IMPROVEMENT PROGRAM
FINAL REPORT
BURGLARY ALARM SYSTEM DEVELOPMENT PROGRAM

Approved


Joseph Meltzer
General Manager
Law Enforcement and
Telecommunications Division

ABSTRACT

This document is a final report covering a burglary alarm survey analysis and the resultant development of a low-cost, reliable burglary alarm system. This program was accomplished by The Aerospace Corporation under contract to the Law Enforcement Assistance Administration. The objective of the development program was to produce a prototype of this reliable, low-cost burglary alarm system and the subsystem components which would be suitable for widespread use in residences and small businesses. The most significant developments of the project are:

- a wireless communication link to and from the sensors,
- a single-point user control at the residence entrance, and
- the use of a low-cost single-chip microprocessor (i.e., a modified deadbolt lock) for implementation of the system logic.

CONTENTS

ABSTRACT	v
SUMMARY	xi
I. INTRODUCTION	1
II. PRELIMINARY DESIGN CONSIDERATIONS	3
A. Background	3
B. Current Systems Designs	8
C. False Alarm Problems	10
D. New Technology	13
E. Problem Statement	20
III. SYSTEMS DESIGN	23
A. Design Approach	23
B. Maximum Performance Design	26
C. Low-Cost Adaptive System	41
D. The SYNCTRAN (Synchronous Transmission) System	62
E. Conclusion	66
IV. SPECIAL REPORTS	67
A. Investigation of Burglar Alarm Sensors	67
B. Performance and Reliability Evaluation of a Passive Infrared Intruder Sensor	97
C. Rossin Corporation Thermal Intruder Sensor	101
V. FUTURE DEVELOPMENTS	107
A. Mod II Adaptive Alarm System	107
B. Central Station Design	118
NOTES	125

ILLUSTRATIONS

1.	Comparison of Current and Proposed Systems	5
2.	Microprocessor Package	24
3.	Overall Concept, Maximum Performance Design	27
4.	Burglar Alarm System Central Processor, Front Panel	28
5.	Internal View of the Central Processor	29
6.	Local Alarm, External Interface and Central Processor	31
7.	Sensor-Transmitter	32
8.	Central Processor Code Plug Board	34
9.	Entrance Control Hardware	37
10.	Total System Package	42
11.	Adaptive Alarm System	44
12.	"Brassboard" or Developmental Sensor-Transmitter	46
13.	Boundary Sensor	46
14.	Rossin Infrared Sensor in Operation	48
15.	Rossin Infrared Sensor with Chassis Partly Removed from Case	48
16.	Specifications of PLS-401 System	49
17.	Features of PLS-401 System	50
18.	Controller, Front Panel	52
19.	Hoffman Receiver Circuit Diagram	54
20.	Symtec Receiver Circuit Diagram	55
21.	Fire/Smoke Detector	57
22.	Hoffman Transmitter Circuit Diagram	58
23.	Symtec Transmitter Circuit Diagram	59
24.	Deadbolt Lock, Outside	61
25.	Deadbolt Lock, Inside	63
26.	Internal Functioning of the Deadbolt Lock	64
27.	SYNCTAN (Synchronous Transmission) Concept	65

ILLUSTRATIONS (Continued)

28.	Doppler Frequency	70
29.	Block Diagram of Breadboard Ultrasonic Alarm Sensor . .	75
30.	Time Histories of Outputs	78
31.	Power Spectral Densities	78
32.	Comparisons of Measured and Computed Mean E-Field Signature Variation with Subject Range from the Detector . .	79
33.	Power Spectral Density (Intruder Velocity 1.3 Feet Per Second)	87
34.	Power Spectral Density (Intruder Velocity 2.5 Feet Per Second)	88
35.	Power Spectral Density (Intruder Velocity 6.2 Feet Per Second)	89
36.	Rossin Corporation Thermal Intruder Sensor	90
37.	Block Diagram of the Aerospace Active Infrared Burglar Alarm	94
38.	The Aerospace Active Infrared Burglar Alarm	94
39.	Rossin Thermal Intruder Sensor, Schematic Diagram . . .	102
40.	Improved Thermal Intrusion Sensor with Two-Beam Mirror .	104
41.	Total System Package for Mod II Microprocessor	108
42.	Seven-Segment Hexadecimal Numeral Display	115
43.	Burglar Alarm System Central Station Display	121

TABLES

1.	Burglar Alarm System — Alarm Outputs	40
2.	False Alarm Test Summary, Conventional Unit	73
3.	Advanced Ultrasonic Burglar Alarm Sensor Parts	
	Count and Costs	75
4.	Statistics Summary	82
5.	System Operating Modes	111
6.	Key Switch Positions	114

SUMMARY

More than 2 million residential burglaries are reported each year, and the number is increasing at a national rate of 12.5 percent per year. Reported losses from burglaries presently amount to \$2 billion annually. The actual number of burglaries and real-dollar losses substantially exceed these reports. It has been confirmed that less than one-third of all burglaries are reported because of fear of reprisal, low individual dollar loss, the inconvenience of travel to police stations or courts, or lack of confidence in the police and judicial systems (the average conviction rate for apprehended burglars is only 8.2 percent).

A. Survey and Analysis

The initial Aerospace effort was a survey and analysis^{*} of the burglary problem, an identification of what particular technology might be applicable, and an estimation of the possible benefits to be derived from applying technology to the problem.

In the course of this survey, it was determined that the typical convicted burglar is under 25 years of age, his methods are unsophisticated, and he could easily be dissuaded from carrying out a burglary by a simple but effective alarm system, or more easily apprehended if such a system were used. It was found that wider use of such systems is inhibited by their high cost and low reliability, and that an excessive false alarm rate is the most detracting operational factor. The survey also showed that if these false alarms could

*"Survey and System Concepts for a Low Cost Burglary Alarm System for Residences and Small Businesses," ATR-74(7904)-1, Reissue A, The Aerospace Corporation, El Segundo, Calif. (August 1976). Prepared for the National Institute of Law Enforcement and Criminal Justice, Law Enforcement Assistance Administration, U.S. Department of Justice.

be reduced to less than one per year, then police resources would be adequate to respond to essentially all alarm calls, even though a substantial number would still be false. It was further noted that most victims of burglaries are low- to middle-income citizens with very limited knowledge of security measures.

1. System costs. Current effective residential systems cost from \$500 to \$2000, and, in some instances, there is an additional \$15 to \$25 monthly charge. Installation represents as much as 50 percent of the total cost.

2. False alarms. Most of the poor reliability (i.e., false alarms) is associated with improper operation of the equipment by the user in over 50 percent of the cases; 20 to 30 percent of the remaining false alarms are apparently caused by the so called "volumetric" room sensors.

3. Communication to a central station. It was also determined from these studies that there was a need to inexpensively communicate alarm data from a residence to the police or central station. Studies and analyses were undertaken by the Stanford Research Institute, under an Aerospace Corporation subcontract, to evaluate alarm transmission media and techniques. It was concluded that only telephone and radio appeared practical.* Aerospace consequently initiated an effort to investigate a new concept called SYNCTAN (Synchronous Transmission), described in Section III-D. of this report.

B. Hardware Development

Hardware development was begun by award of a subcontract to GTE/Sylvania Incorporated for development of a maximum performance, integrated

*S. Scala, et al., "External Alarm Transmission Evaluation," Final Report, P.O. 44365-V, Stanford Research Institute, Menlo Park, Calif.

burglar alarm system using powerlines as the internal communication medium.* A description of this system is provided in Section III-B. of this report. Parallel Aerospace efforts were made to investigate all types of sensors applicable to a low-cost burglar alarm system and to develop a minimum-cost system design using radio as the internal communication medium.

C. Adaptive Alarm System Concept

Efforts in 1976 were devoted almost exclusively to hardware development. The object was to explore new hardware concepts that were inherently low cost and had the required reliability. The efforts were not directed toward any specific system, but rather to the development of hardware ideas and guidelines that industry could pick up and commercialize. The most significant results were:

- A low-cost, reliable thermal intrusion device
- A miniature radio link connecting sensors to a central controller
- A low-cost microcomputer controller
- A single-point user control from a deadbolt lock at the entrance

The Adaptive Alarm System is intended to be flexible for both the manufacturer and the user, and, since it is not being designed for a particular manufacturer, one may expand on the basic system design to optimize the manufacturing process or enhance the marketing appeal. The system is designed for the low-priced market and aimed at low- to moderate-income homeowners. This is achieved through a low-cost microprocessor design and through the wireless architecture, which reduces installation costs. A principal objective is to reduce false alarms by simplifying the system's operation

* "GTE/Sylvania Burglar Alarm System Final Report," No. E-247, GTE/Sylvania Incorporated, Mountain View, Calif. (September 1976).

to the homeowner, yet still making it effective at low cost through the use of large-scale integrated (LSI) circuitry techniques.

This wireless burglary alarm system may include up to 32 miniature radio sender modules that may be located at locks, windows, doors, indoor floor switchmats, or incorporated in other detection devices, such as ultrasonic motion sensors or fire detectors. The controller, incorporating a microprocessor and a radio receiver for detecting the radio module output messages, will accomplish a prescribed logic sequence, generating output signals to a local alarm (a bell), a display, a telephone, and responding to other operating controls (i.e., test switch, tamper switch, etc.).

Each radio sender module transmits a unique 15-bit permanent identification code and a 1-bit status message as a binary sequence (16 bits total). The microprocessor in the controller will recognize the identification code of each of the sender modules associated with one system. Subsequently, the triggering of any radio-sender modules will be detected by any alarm receiver located within a distance of 40 to 50 feet from the sender, but only the controller that is programmed for this particular sender code will react to this transmission. At least 32,000 sender code combinations exist; therefore, the probability that more than one alarm system will respond to any specific radio sender module will be negligible.

Deadbolt locks at entrances to a residence control the alarm system. A resident must only lock the door to arm the alarm system, or unlock the door to disarm the system. A remote disarm switch may also be used to disarm the system. The system distinguishes inside arming from outside arming. When arming the system, an audio alert signal is transmitted to the resident if any sensor was left open prior to arming. If not corrected, however, the open sensor will be ignored, i.e., will not generate an alarm condition, and the controller will fall back to its best operating mode, excluding that sensor.

User controls are intentionally simple: a fire alarm reset button, a test button, and a single character light-emitting diode (LED) display, which identifies each sensor by an assigned character, are located on the front panel of the controller. Users assign channel numbers to their sensors during initial system installation or subsequently when new sensors are added.

The LED display allows a total of 32 distinct patterns represented by a hex character and an optional decimal point. Each particular display represents a distinct channel that is associated with one particular class of sensors. The particular classes of sensors (channels) include boundary sensors, internal sensors, emergency sensors, fire sensors, auxiliary emergency sensors, auxiliary control sensors, and arming/disarming sensors. Thus, when locking or unlocking the front door, the particular channel to which that sensor is assigned will be displayed for a short time. During an alarm sequence, the channel causing the alarm will be displayed whenever the display would otherwise be blank.

In addition to the above functions, the seven-segment display will flash for 20 seconds, displaying any open sensors upon locking the door (i. e., arming the system). Accompanying this will be an audible alert to let the resident know that an unsecure condition exists.

An alarm bell is included in the system for local notification of a burglary, fire, or other emergency. The fire alarm is differentiated from the continuous burglary and emergency bell by a pulsating bell of approximately 2 Hz with a 50 percent duty cycle. All alarms continue for a maximum of 15 minutes, but may be turned off at any time by disarming the system.

Additional outputs from the microprocessor are available to control auxiliary functions. These latched lines, set by auxiliary channels and through the use of extra circuitry, may operate house lights, garage doors, etc.

Central station equipment has not been designed, although the basic elements of such design have been considered to ensure that a technically and economically feasible design could be evolved that would be compatible with the Adaptive Alarm System operation.

1. Individual components. The components of the Adaptive Alarm System are described below.

a. Intrusion sensor. The basic design of this system is the product of the Rossin Corporation of Santa Barbara, California. A simple version of their design has been on the market for over a year. Aerospace evaluated the design and determined that it was reliable and inherently low in cost, although it lacked certain features believed to be necessary to increase its detection probability. Changes were also necessary to permit communication via wireless means to a central controller located in another part of the household.

A subcontract was let to Rossin Corporation for these improvements. The main improvement was a simple mirror arrangement wherein the original single detection beam could be split into two separate beams. For example, one beam could be pointed down the hallway and the second beam pointed through a living room. The final product consumed a current under 5 microamperes, and, using lithium batteries, this device could be installed on a wall and operate there unattended for up to 10 years.

b. Internal communications. A wireless, internal communication system was desirable to reduce installation costs. Anticipating that a low-cost system would result in alarm proliferation, with a large amount of crosstalk adding to the false alarm problem, means were sought to minimize the possibility of crosstalk in such areas as an apartment complex where 50 or more sensor-transmitters might be within range of each other in different resident units.

Two basic approaches were investigated: (1) a digital coding technique providing up to 32,000 different codes, and (2) a limited distance transmitter that exploited "near-field" radiation phenomenon. Models of the latter phenomenon reveal that, within the near field, certain terms in the radiation equation drop off very rapidly with distance as compared with the so called far-field term normally employed in radio communication systems. Furthermore, in the near field these fast-dropping terms are substantially greater in strength than are the far-field terms. Therefore, one obtains a high energy radio-frequency volume immediately surrounding the transmitting element, but this rapidly drops off with distance. By proper choice of radio frequency, one can take advantage of the near-field effect to limit the radiation distance to within a prescribed volume.

Equipment was constructed and tested using both the digital coding technique and the near-field concept; both were successful. In the case of the near-field devices, a probability of detection in excess of 95 percent was achieved at distances of 35 to 40 feet, but this probability was reduced to near 0 at distances exceeding 60 feet, as desired. Using conventional radio techniques (as employed today), the probability of signal detection would fall off more slowly. For example, a 95 percent probability at 40 feet might only reduce to approximately 85 percent at 60 feet, and such systems would consequently suffer more interference because of other transmitting devices in the vicinity. Either the near-field or the digital technique, or both together, appear promising for future applications.

c. Adaptive controller. The third subtask involved an investigation of new controller techniques and better logic arrangements to reduce the probability of user-caused false alarms. It was determined that the best results would be achieved if the user had only a single control and if this control could be exercised by the user in his normal living routine.

The preferred solution is a deadbolt lock at the front entrance that would turn the alarm system on and off as the user left or entered the house. A special lock was required for this purpose, and a subcontract was let to the National Lock and Hardware Co. in Rockville, Illinois, to develop such a device. The requirement placed on this company was that the resulting lock must be essentially identical to the commercial lock that they currently sell through Sears Roebuck and Co. and other channels, and any modifications must be simple and reliable and not add significantly to the cost of the end item.

National Lock was successful in achieving the specified goal and delivered 10 locks modified as requested by Aerospace. Limited on/off cycle testing indicated a 100-percent operating reliability when the lock is combined with a special Aerospace designed electrical interface logic circuit.

d. Microprocessor. Probably the single most significant breakthrough of the entire program was the very low cost microprocessor design. At the time of task termination, the second version of this microprocessor (Texas Instruments TMS-1000) was approximately 50 percent complete. Within its single chip, the microcomputer contains a clock, 1024 words of read-only memory, 64 words of random-access memory, a program counter, an accumulator, a code converter, and several other housekeeping registers, as well as output latches for both addressing purposes and for an off-board digital display. The quoted price for this microcomputer is \$3.10 in quantities of 50,000.

D. Conclusions

Numerous presentations were made to persons in alarm industry associations and to individuals with alarm companies who visited Aerospace to review this technology. The general opinion of these industry representatives is that the Aerospace effort represented a significant contribution to alarm

technology and resolutions, and letters to this effect have been published and distributed by them. It is believed that the technology developed in this program can and will have a significant impact in reducing both the cost of an alarm system for residential and small business use and the likelihood of false alarms.

CHAPTER I. INTRODUCTION

Burglary is a severe and growing national problem that causes enormous financial losses annually. The effects of burglary are particularly severe in low-income areas and among small businesses. To combat this problem, the Law Enforcement Assistance Administration initiated a program in 1973 to evaluate the actual magnitude of the problem and develop an effective means of combatting it. This is the final report on that effort, and it documents the development of a reliable, cost-effective burglar alarm system especially applicable to low-income residences and small businesses. This system was originally conceived and studied by The Aerospace Corporation, under the sponsorship of the Law Enforcement Assistance Administration, during fiscal year 1974. Hardware and software development continued through fiscal year 1976 and culminated in the testing and demonstration of a low-cost, adaptive burglar alarm system suitable for widespread use in residences and small businesses. The system includes the following:

- A thermal intrusion sensor
- A controller with low-cost microprocessor and related programming instructions and controls
- Optional wireless or semiwireless sensor-to-controller internal communication modules
- Optional phone dialer or radio external transmission system for communication between the residence (or business) and a response point (police or other central station).

This report documents the background investigations and accompanying market survey, the preliminary design considerations, the resulting system design, and research and development activities. It then describes a maximum performance design and the application of advanced technology to production of a prototype low-cost system. The report concludes with a discus-

sion of future developments that may affect both the improved performance and the increased cost-effectiveness of the proposed system.

The central objective of these activities was to reduce the incidence of burglaries through the development of a low-cost, highly reliable burglar alarm system. Concurrent objectives included reducing false alarm signals to the minimum, developing low-cost sensor systems to detect human intrusion, providing an inexpensive means of transmitting alarm data both within the protected area and to exterior response agencies, and developing an integrated control system that could be easily installed and simply operated by the user.

This report represents the culmination of the development effort accomplished by The Aerospace Corporation. The next phase would have been a field test in which approximately 500 production-line systems would have been put into use.* However, the program was terminated by direction of LEAA on 20 August 1976. Through presentations to and personal contact with members of the alarm industry, the general opinion was that Aerospace concepts and development represented a significant contribution to alarm technology.

*"Burglary Alarm System Field Test - Final Report," ATR-77(7617-23)-1, The Aerospace Corporation, El Segundo, Calif. (March 1977). Prepared for the National Institute of Law Enforcement and Criminal Justice, Law Enforcement Assistance Administration, U.S. Department of Justice.

CHAPTER II. PRELIMINARY DESIGN CONSIDERATIONS

A. Background

The Aerospace Corporation entered this program in September 1972 under a task sponsored by the Law Enforcement Assistance Administration and administered by the Equipment Systems Improvement Program, and completed a survey and concept definition during fiscal year 1974 on a cost-effective burglar alarm system for low-income residential and small business applications. Development of the resulting concepts was begun in fiscal year 1975.

The initial study and survey^{1*} addressed the crime of burglary and the question of whether any alarm system at any cost offered sufficient protection to justify its development. The evidence brought forth the following conclusions:

- Alarm systems are highly effective in reducing financial losses from burglary.
- Burglar alarms offer the only proven solution for reducing the amount of unreported crime and increasing the arrest rate of offenders.
- Because burglary is now considered a career, an increased arrest probability resulting from a proliferation of alarm systems will have a multiplying effect on the decreased burglary rate.

Urban and suburban residents and small businesses are most in need of protection against burglary. Residential offenses have reached 63 percent of the total of all burglaries, with dollar losses increasing 17.7 percent each year for the past 12 years. The average large-city resident can expect a 10.8 percent probability of being burglarized within the year, with an average loss of \$315. The evidence shows that only one-third of these crimes will be reported to the police, and so many of them will be reported late that only 8.2 percent of such crimes will result in a guilty-as-charged verdict.

*Numbers refer to Notes on page 125.

Rural crime rates, although increasing, are not on the same scale as urban and suburban burglaries. Burglar alarm systems in rural areas are less effective as a deterrent because of the longer response times by law enforcement agencies and the generally lower probability of burglary outside cities and towns.

The use of alarm systems in even the most burglar-prone areas has been inhibited by two factors: (1) Most systems cost \$100 or more for installation of the purchased equipment, thus imposing an additional economic restraint on those who need them; and (2) the design of the systems available have been prone to error, causing too many false alarms that demand police response.

Significant improvements in interior sensor design, human interface engineering, automatic error detection, and communication technology should produce equally impressive improvements in deterrence and apprehension. Any value, however, for an acceptable cost and false alarm rate reduction must be determined by the particular application.

In the course of the initial study, an examination of burglary statistics showed that an increased use of improved alarm systems offered a number of appealing possibilities. These are shown in Figure 1. (See Note 1.)

1. The cost-effective burglar alarm system. The foregoing conclusions led to a conceptual system design called the Cost-Effective Burglar Alarm System. The system development program ran in two parallel paths:

- A more sophisticated, maximum performance system of potentially high cost, using a semiwireless powerline intercommunication system.
- A minimum-cost adaptive system, using coded near-field radio techniques for intercommunication.

The basic system concepts of both paths included at least one simple sensor capable of discriminating between human motion and other potential

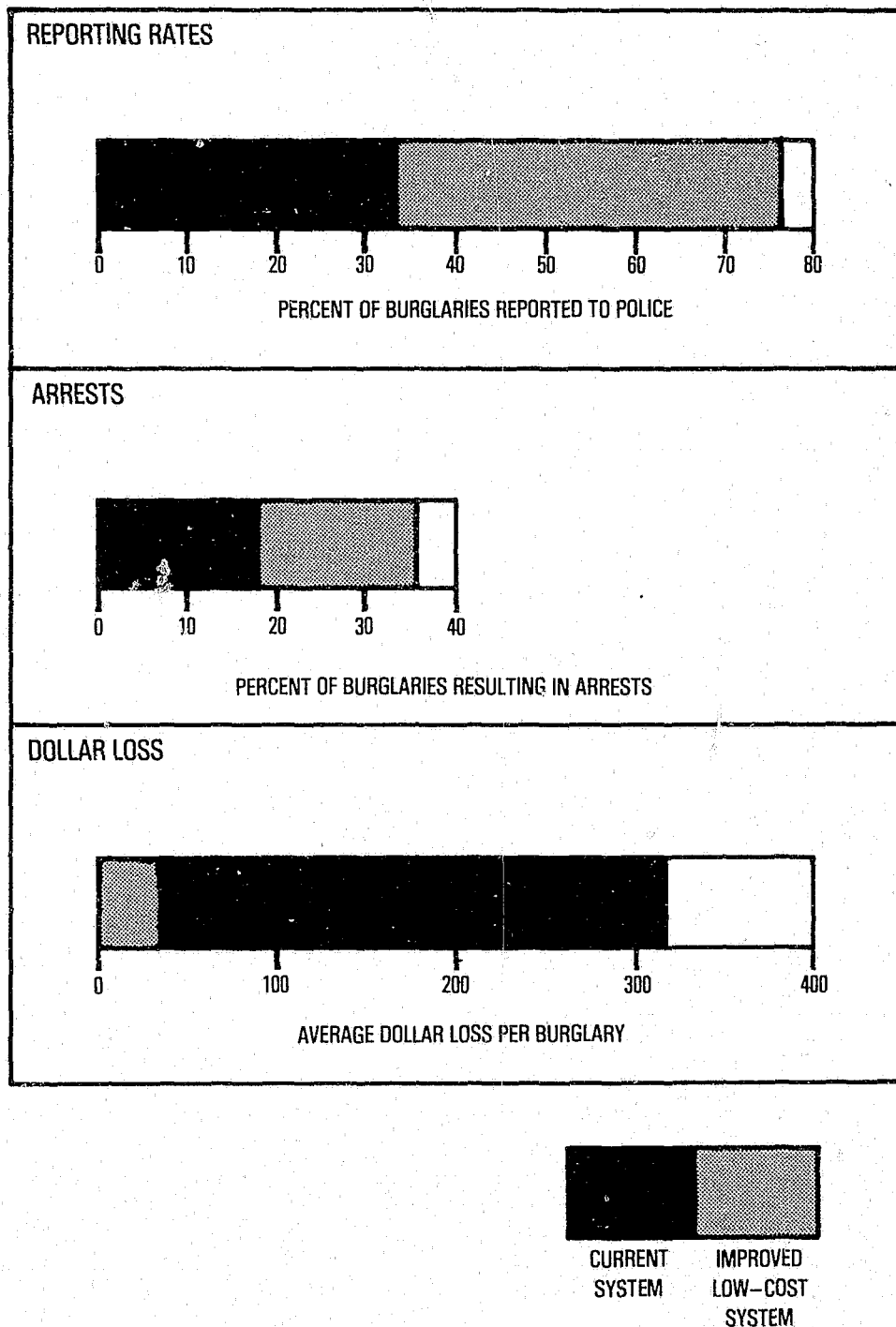


Figure 1. Comparison of Current and Proposed Systems

alarm sources; a low-cost processor with logic to improve reliability and operation; and an integrated door lock under system control.

The door lock control is a very important factor in reducing inadvertent user-caused alarms.

The system concept provided for indicating an intruder through a local alarm, through a silent automatic message to a central station, or both.

2. Market survey. The maximum performance system resulting from the study showed how modern technology could be applied to the problem, and how certain capabilities would not be available at any cost. Concepts for an effective low-cost system were developed, and the potential market among the general public and small businesses in high-crime and high-population-density areas was determined by a market survey. The survey was designed to define the level of public concern with burglary, obtain consumer reactions to the low-cost system concept, and assess the acceptable price levels.

The market survey was based on one Standard Metropolitan Statistical Area (SMSA) in each of the following nine census regions:

- Boston, Massachusetts
- Paterson-Clifton-Passaic, New Jersey
- Chicago, Illinois
- Kansas City, Missouri; Kansas City, Kansas
- Charlotte-Gastonia, North Carolina
- Nashville-Davidson, Tennessee
- Dallas, Texas
- Denver-Boulder, Colorado
- San Francisco-Oakland, California

The results of the survey showed a positive potential for the burglary alarm system among both residents and businessmen. The statistics obtained are summarized in the following list:

- Forty-one percent of heads of households rate home burglary as a serious problem in their neighborhoods. Thirty-two percent have already been victims of burglaries or burglary attempts.
- Only 4 percent of these households currently have a home burglar alarm system.
- Twenty-four percent say they would be very likely to purchase such a system if it were within the \$200- to \$300- price range.
- Among businessmen in high crime SMSAs, there is also a potentially good market for the product.
- Sixty-four percent of the businessmen considered burglary a serious problem in their neighborhoods. An identical proportion (64 percent) had been the victims of burglaries or burglary attempts. However, over half of the businesses (56 percent) already had a burglar alarm system.
- Even so, purchaser interest in the new system was relatively high, with 13 percent very likely to buy at \$500, 8 percent more likely at \$350, and an additional 16 percent very likely to buy such a system at \$200. This represents a total of 37 percent of the businessmen who said they are very likely to purchase the system within the likely high and low range of the probable selling price.

3. Conclusions. The conclusions from the study and survey are presented in the following list. They support the development of a highly reliable, low-cost alarm system.

- A need exists for a low-cost, reliable security alarm system for low-income residents and small businesses.
- A need exists for new and/or modified alarm response tactics.

- The need exists to integrate burglar alarm systems and their components with other crime-fighting strategies.
- The need exists for a reliable human-discriminating intrusion sensor to reduce the magnitude of sensor-induced false alarms.
- The need exists for the definition and development of new or modified alarm communication methods.
- False alarms are a key problem with existing alarm systems because of the nondiscriminating features of sensors and the poor human engineering of control systems.

B. Current Systems Designs

There are many companies marketing burglar alarm systems for homes and small businesses, offering a wide variation in price and complexity. The types of motion detectors include ultrasonic, infrared, microwave, audio, vibration or shock detectors, and magnetic sensors, with ultrasonic systems predominant. Few of these, however, are people-discriminating. Application of new technology, such as metal-oxide semiconductor and large-scale integrated circuitry, or coded digital transmission, is rare. In general, the military services are the primary motivating and funding source for innovative sensor systems, with business and industry principally concerned with improving known systems, such as radio frequency, infrared, and ultrasonic devices.

Hard wiring is the most common medium for internal transmission, although a few systems use radio frequency techniques or indoor powerlines. Combination door lock and alarm controls are under consideration by some manufacturers, but are not in the current inventory.

Telephone lines are the most common medium for external signal transmission. The majority of systems use low-quality leased lines, a few require voice-grade lines, and some are equipped with line seizers that use the subscriber's normal telephone line. Automatic dialers are occasionally offered

as an add-on feature to the more expensive systems, but they have a history of high false alarm rates. Some radio frequency systems are in use, including Law Enforcement Assistance Administration - funded experiments with transmissions to police centrals or squad cars; such systems, however, are subject to interference, equipment reliability problems, and a lack of verification of system operability.

Current costs for systems of reasonable reliability range from \$500 to \$2000 for residences and from \$500 to \$3000 for small businesses; service or rental charges are from \$15 to \$50 per month. Most integrated control systems are too expensive for average home use.

Central station (response) systems are both complex and expensive, designed for large businesses, institutional use, high-income residential areas, or government installations. Central station equipment used by the police and private alarm companies varies considerably as to techniques, designs, and displays, with many installations discredited because of low reliability.

Deficiencies of existing alarm systems are summarized as follows:

- The wireless systems are subject to false alarms from crosstalk with other systems in close proximity.
- Most systems cannot identify which sensors sent an alarm signal.
- There are no integrated, low-cost cooperative phone dialers as part of an alarm system.
- The systems do not alert the user to a specific unsecure condition when leaving the residence or business.
- Low-cost systems have little or no logic protection from user-caused false alarms.
- The costs of current systems are beyond the range of most potential users.

C. False Alarm Problems

False alarms are the largest problem of burglar alarm systems. Numerous studies imply that police respond to anywhere from 9 to 49 false calls for every true (actual burglary, or attempt) alarm. The experience of most communities is that 10 percent or less of the alarms received are due to an actual burglary. It must be accepted that any sensing device will give a false signal occasionally, and this includes burglar alarms. Police departments will usually accept a high number of false calls, just as they accept false leads in the process of solving a crime, as a characteristic of law enforcement work. When, however, the number of false alarms consistently exceeds the number of true signals, the system becomes an aggravation, and the attitude of the responders to that system becomes increasingly negative. A substantial increase in the number of burglar alarm systems in a community would, under present circumstances, enormously increase the number of false alarms demanding unproductive police response in each instance. Any consideration of expanding the use of burglar alarm systems must, therefore, address the critical problem of false signals and include actions to reduce them. This requires an understanding of how false alarms are categorized and tallied.

1. Categorizing alarms. The Alarm Industry Committee for Combating Crime has divided true and false alarms into several categories. True alarms are those that result from actual, or attempted, unauthorized entry, including those alarms detected through property damage and the opening of doors or windows by wind or storm. The rationale for this broad definition is that the system should detect and announce any reduction of its ability to protect the premises, even those resulting from natural causes.

The Alarm Industry Committee for Combating Crime groups false alarms into three areas: externally caused alarms; equipment failure; and internally caused alarms.

a. Externally caused alarms. External alarms are those caused outside the protected area, such as telephone lines leading to the central station, or at the response agency itself.

b. Equipment failure. Equipment failure alarms are those resulting from a malfunction of installed equipment.

c. Internally caused alarms. These alarms occur inside the protected area and are generally caused by the user's operational error or neglect (such as forgetting to disarm the system on entry). Internal alarms are the principal cause of false alarms, and can be attributable to both lack of care in using the system and inadequate human factor protection in the system design.

2. Measuring false alarm rates. In considering the number and proportion of false alarms, as compared with true alarms, it is necessary to define the measures used. Until recently, the method most used was to express the ratio of false alarms to the total number of calls: for example, a false alarm ratio of 50 percent implies that there was one false alarm for every true one; a ratio of 90 percent implies that 9 out of 10 calls were false. In many cases, this method was misleading because it reflected the local burglary rate as well as the reliability of the local alarm system, resulting in distorted comparisons between communities with different burglary rates. Where the primary concern is measurement of system quality in terms of alarm reliability, the ratio method can be deceptive. This has led to the generation of two newer terms: "false alarm rate," and "mean time between false alarms."

a. False alarm rate. The false alarm rate is the average rate at which false alarms are received from each installed system. A system that errs twice a year has a false alarm rate of two.

b. Mean time between false alarms. The mean time between false alarms shows the average time between false alarms received from a desig-

nated installation. A system that errs twice a year (a false alarm rate of two) would therefore show a mean time between false alarms of 1/2 year.

3. Acceptable false alarm rate. No official position has been taken on what an acceptable false alarm rate should be. It is known, however, that law enforcement officials, in general, consider the number of responses to false alarms unacceptably high when compared with the number of true calls received. There is an understandable concern that a large increase in the installed number of alarm systems that are no better than the existing ones could lead to an unacceptable number of false alarms and either overwhelm police resources attempting to respond or cause them to disregard the massive number of calls received. However, burglary is the largest single crime in the United States, and the average urban home or business has a 10.8--percent probability of being attacked in any one year,¹ with an average certainty of being attacked once in each decade; the annual dollar loss to burglaries is approaching \$1 billion.

The desirable effect of increased burglar alarm systems can be accompanied by the undesirable effect of further increasing false alarms, already occurring at a rate unacceptable to many police departments. One of the preliminary design considerations, therefore, is to ensure that any system developed will contribute to a reduction in the existing mean time between false alarms, now ranging from 0.29 year to 0.48 year in a number of representative cities examined.¹ Although no standard has been set as to what false alarm rate would be acceptable, there is reason to believe that a doubling of the better rates now obtained (to a mean time between false alarms of about 1 year instead of 0.48) would be tolerable with the increase in the number of systems. This rate appears achievable if significant improvements are made in sensor performance, arming and disarming techniques, and the reliability of transmitting alarm data.

Because the majority of false alarms are internally generated through user error or neglect, the human interface is the most likely area for substantial gains in system reliability. The design must compensate for the human factor to a greater degree than at present, rendering inadvertent activation virtually impossible and warning the user prior to transmitting the alarm message. The logic of the system should require a sequence of events to occur prior to sending an alarm, based on sensors or stemming from situations likely to be false inputs. In combination with the more mechanical improvements to be made in externally caused alarms, and the elimination of equipment malfunctions, such actions are likely to realize the general design goal of extending the mean time between false alarms to more satisfactory intervals. The resulting design should be as simple as possible — using human engineering to reduce user error, human-discriminating sensors, and automatic detection of equipment malfunction.

D. New Technology

Building the required intelligence into a burglar alarm system and meeting the cost goals established requires the latest technology available and the application of old technology to new uses.

New and different technology is most applicable to the control system, the internal communication, and external communication.

In the control system, intelligence and logic are required at low cost. An initial consideration was the development of a large scale integration (LSI) circuit to be used as the logic for control of the system. The reality of the microprocessor, which is more versatile and does not take the large front-end investment needed to develop an LSI chip, superseded the original thought, and it was decided to use a microprocessor in the system.

Microprocessors are the central processing unit portion of a computer on a chip. A microprocessor chip (or chips) together with memory chips and

input-output chips qualifies as a microcomputer and is available now on a single printed circuit board. The microprocessor chip has evolved from efforts to generalize chip design to provide sufficient flexibility in handling application variations through programming. As integrated circuit manufacturers continue to make major advances in semiconductor chip products, the concept of a central processing unit on a chip was inevitable.

One significant new concept that has evolved with microprocessors is the use of random-access memories and read-only memories. The random-access memories are used for data storage and scratch pad, whereas the read-only memories are used to store the instruction sequences. Since the environment for microprocessors is typically dedicated applications, the random-access memory and read-only memory capacity requirements can be explicitly defined, based on the partitioning of programs and data. Input-output is the last obstacle now being addressed by integrated circuit manufacturers to make available a full line of interface chips for off-the-shelf microcomputer implementations. Input-output interface chips are the hardest to standardize because of the large number of types that potentially need to be accommodated.

Microcomputers are available from the following three kinds of suppliers:

- The integrated circuit manufacturer offering a kit including the microprocessor, the memory, and an assortment of input-output interface chips.
- The minicomputer manufacturer with special or standard chips to implement a unit instruction set compatible with existing minicomputers (i. e., re-implementing the minicomputer).
- System houses that build a microcomputer for specific applications, using either microprocessor chips or standard transistor-to-transistor logic chips built as a microprogrammed type of control circuit.

Functionally, the microprocessor includes the arithmetic logic unit, the general purpose registers, and the control-bus structure. The architecture is to some degree dependent on the partitioning of the microprocessor between one or more chips, the package pin allocation, the chip size, and the off-chip memory and input-output bus structure.

1. Architecture

a. Word length. Word length is a starting point from which to discuss the various microprocessor designs. Word length is a meaningful characteristic because it usually relates to application. For instance, calculator chips are 4-bit for decimal digit operations, whereas communication terminals are 8-bit for character transmission codes. Base instruction sets are increased in number by additional modes or extensions. The number of instructions is not as significant as the applicability of the instruction set to the requirements for the intended application.

b. Speed (throughput). Speed or throughput is very dependent on architecture. The smaller size microelectronics are slower because the microprocessor chips have a pin limitation that does not allow parallel input/output for faster operations. Fewer pins mean less information on what is happening internally and what should happen externally. Therefore, more encoding is done because of fewer signal pins, and decoding is necessary off the microprocessor chip to get the job done. Clock speed (or frequency) is not necessarily indicative of execution speed. Speed is a function of data and address-path widths, number of separate paths, and overlap in the fetch and execute cycles. As an example, the Intel 4004 uses a 750-kHz clock and the Rockwell PPS-4 uses 200-kHz four phase, yet the PPS-4 does some computations faster.

c. Arithmetic and register operations. Arithmetic and register operations in microprocessors have evolved into a capability for both decimal and binary arithmetic. Because of the pin limitation of the off-chip memory,

most microprocessor architectures use a push-down stack feature of some sort. The push-down stack helps the programmer to minimize register transfers, facilitates counting and sorting, and limits needless transfers to and from main memory. The push-down stack is a last-in, first-out buffer that retrieves data in the reverse order from which they were stored. The use of push-down stacks provides a convenient means for handling register manipulations and minimizes the number of memory reference accesses to do certain programming operations. Stacks usually consist of registers built into the processor. The stack size is usually limited to a fixed number of registers, but some of the newer designs (e.g., Intel 8080) use random-access memory locations for the stack, but the pointers must be maintained by the software.

d. Memory section. The memory section of a microcomputer usually accounts for a major portion of the chips. Random-access memories are used primarily for variable data and they are relatively expensive compared to read-only memories. Read-only memories do have mask charges so quantity is needed to justify the cost and production delay time involved. The random-access memory and read-only memory chip devices have to be mated to the address/data bus structure of the microprocessor chip to be efficient parts in the microcomputer operation. In the 4-bit microprocessors, memory chips were tailored to the address/data structure with special chips. The 8-bit microprocessors use either special memory chips, or standard read-only memories and random-access memories, depending on the manufacturer. The latter approach allows multiple sourcing of parts and more competitive pricing. For obvious reasons, programmable read-only memory chips have become popular when small quantities are involved. One type of programmable read-only memory can be erased by an ultraviolet light so that it can be reprogrammed without removing the chip from the assembly. Other kinds

of programmable read-only memories (e. g., diode fusible link) are programmed by a burn-in technique using either an accessory kit or by sending the chip to a service bureau.

e. Design. The first microprocessor chips were the 4-bit machines used primarily in calculator products. Two of the popular devices available in this category are the Intel 4004 and Rockwell 10660. Even though these designs were for parallel operation on 4-bit decimal digits, they have sufficient general-purpose computer design flexibility to be effective in many other kinds of applications. Their instruction times range in the order of 5 microseconds to 20 microseconds. The designer-programmer must be familiar with the microprocessor instruction timing to effectively program it into the application. Each instruction execution has one or more cycles to complete execution when each cycle has three or more states. Each state is composed of several subinterval states driven by the system clock. Some of these first 4-bit microprocessors required the designer to provide off-chip registers to address memory, decoders to synchronize operations, and a clock generator. Then the integrated circuit manufacturers came out with complete microprocessor chip designs (e. g., Intel MSC-4 and Rockwell PPS-4) to eliminate this problem for the designer-programmer.

One important variation to the fixed word length 4-bit microprocessor designs is the building block design with either 2-bit or 4-bit slices that can be used to build up 8-, 12-, 16-, 24-, and 32-bit-wide microprocessor architectures. National IMP-16, an example of this modular approach, has 4-bit slices that can be used to build up the registers, arithmetic logic unit, and input-output data lines to 32-bit widths. This concept is not a new one, but software support and input-output interfaces for all models have not been practical in the past.

The 8-bit microprocessor chips became available in 1972, and interest in them has since increased. The units are characterized by more complex designs, larger chips, and 40-, or 42-pin packages. The longer word length for both addressing and instructions provides higher throughput and easier programming, while the shorter 4-bit word length uses less hardware and smaller memories. Probably, the most useful advantage of 8-bit microprocessors is the additional storage capability (65,000 bytes versus 16,000 bytes for the 4-bit microprocessors). These 8-bit microprocessor designs are very close in architectural features to minicomputers. The direct memory access channel capability permits faster input-output data transfer speeds. The basic approach is to bypass the microprocessor registers to provide direct access to the memory bus. Another significant feature included in some of these microprocessors is a vectored interrupt capability. A vectored interrupt actually provides the address of the routine to be initiated via an indirect jump instruction. The prior program status is saved in a well-disciplined procedure facilitated by the hardware. The typical number of separate interrupt lines that can be accommodated is four or more.

The newer 8-bit designs are referred to as the second generation in microprocessors. These second generation features include the following:

- Separate address and data bus lines
- Multiple address modes (e.g., direct, indirect, relative, and indexed)
- More instructions
- More versatile register stack operation
- Vectored interrupts
- Direct memory access
- Standard random-access memory and read-only memory

All of these improvements have provided a speed improvement of from 20 microseconds to 2 microseconds for typical execution times in going from a first generation microprocessor to a second generation microprocessor.

To complete his microcomputer product line, each manufacturer tries to offer a complete line of input-output interface chips. Standardized interface chips are not possible because the nature of the microcomputer interface and input-output instructions vary significantly from one system to another. The interface chip makes the metal-oxide semiconductor (MOS) voltage levels compatible for transistor-to-transistor logic voltage levels. Interface chip designs tailored to a particular microprocessor input-output structure save the designer-programmer time in development and reduce the overall number of chips needed to make the microcomputer. Functionally, the interface chip accommodates any differences between the microprocessor and the peripheral timing and control logic. If many devices are connected to the same set of input-output lines, transistor-to-transistor tri-state logic provides a convenient way to accommodate these devices. The next step is to make the interface chips parameter selectable so that several models of one kind can be handled with one interface chip.

f. Current developments. Several 12-bit and 16-bit microprocessors are available, and many more have been announced. A few minicomputer companies have introduced a program-compatible microcomputer built around LSI chips. If it is instruction-set-compatible with an existing minicomputer, then the software support of the minicomputer can be utilized. The real impetus for microprocessors is in their application when the cost of minicomputers is too high; the lower-cost microprocessors open up tremendous new possibilities. If, however, the 8-bit microprocessor can do the same job as the 16-bit microprocessor, then it is not clear how much impact the 16-bit architecture will make. There are also variations on the 16-bit

machine (such as 8-bit memory, instructions consisting of both 8-bit and 16-bit word formats, and 8- or 16-bit input-output). Whether 8-bit or 16-bit machines predominate may be more a matter of semantics than a significant difference in architecture.

g. Summary of microprocessor architecture. Microprogrammable architecture is a very practical approach for microprocessor designs. The primary advantages of putting the instruction set in control store memory are cost, open-ended design, and high utilization of LSI standardized products. Since, in many cases, these 16-bit microprocessors would be emulating minicomputers, a microprogrammed architecture would facilitate these goals nicely and would allow the manufacturer a base from which to develop a new machine. These advantages, however, are not without some penalties. For example, when special instructions or functions are put in the microcode, the user has to change the support software (such as assemblers) to accommodate additions to the standard product.

E. Problem Statement

The following list summarizes the problems defined in current burglar alarm systems:

- The false alarm rate is unacceptably high for effective law enforcement operations.
- The false alarm rate is a deterrent for broader use of burglar alarm systems.
- The mean time between false alarms is unacceptably low at values below 0.50 year and must be raised to about 1 year to be tolerable to either the police or the users.

- Current equipment has an inadequate data link error rate, insufficient human engineering to reduce human error, a lack of human-discriminating sensors, and an insufficient automatic detection of equipment malfunction.
- The costs of existing systems are too high for widespread use in urban residences and small businesses.
- Current equipment, both at the user level and in response stations, is too complex and diversified for broad general use.



CHAPTER III. SYSTEMS DESIGN

A. Design Approach

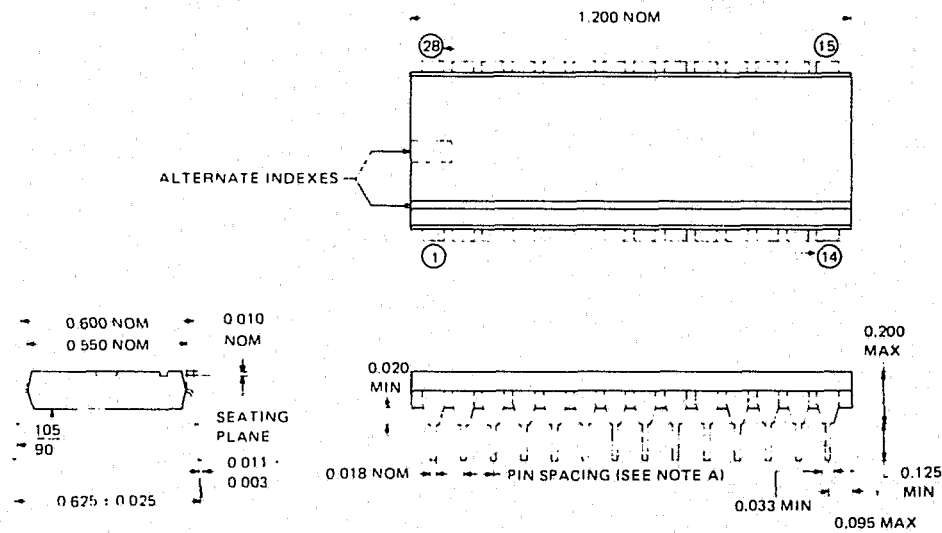
The design approach was to resolve the problems (stated in Section II-E) with a system cost to the consumer of \$200 to \$300. The heart of the system would be a controller that would communicate with the various sensors and control inputs, exercise logic in determining an alarm condition, and execute the alarm announcements accordingly. Using the latest technology, as discussed in Section II-D., a single-chip microprocessor was selected as the least expensive and most applicable solution.

The microprocessor (Fig. 2) monitors inputs from each of the sensors and the entrance control unit, determines the operational configuration and status of the system, outputs signals in proper time and sequence to local warnings and alarms, and communicates to the central station response agency. The logic of the controller will discriminate between false and true inputs and inaccurate operator control, in order to reduce the frequency of false alarms.

1. Inputs. Types of inputs to the controller are as follows:

- Perimeter inputs — Located at doors and windows; may be window foil, vibration sensitive, or magnetic reed switches.
- Internal inputs — For detecting the presence of an intruder within the premises; may be floor switchmats, ultrasonic, infrared, photoelectric, or microwave.
- Panic button input — A small emergency device carried on the person or located at the bedside.
- Fire and smoke input — Detectors to activate a fire alarm; designed to operate through the burglar alarm system in both armed and disarmed states.

TMS1000NL-28-PIN PLASTIC PACKAGE



- NOTES:
- The true position pin spacing is 0.100 between centerlines. Each pin centerline is located within 0.010 of its true longitudinal position relative to pins 1 and 28.
 - All dimensions are in inches unless otherwise noted.

Figure 2. Microprocessor Package



- Entrance control input — A door device to inform the controller whether the door is locked and to define whether it was locked from the inside or the outside.
 - Auxiliary input — A user convenience separate from burglary and emergency inputs; it may be used to monitor and report on equipment failures within or about the premises and thus avoid resulting property damage.
2. Outputs. Types of outputs from the controller are as follows:
- Light-emitting diode (LED) display — Output to display panel showing status of system.
 - Local warning/alert — Output to a small, built-in, audible device to warn or alert the user that an alarm is imminent, or that there is an unsecure condition.
 - Local alarm — Output to a large, audible device on the premises, an option available to the user.
 - Central station — Output to the response agency in the form of alarm and system information; sent via landline or radio.
 - Auxiliary — Output to special service features (appliances, garage doors, lighting).

3. Maximum performance design. The purpose of this design was to bring together as many of the needed functions as possible for maximum performance. Undertaken by GTE/Sylvania Incorporated, the result was a sophisticated, entrance-controlled, powerline communications alarm system. This design is described in detail in Section III-B.

4. Low-cost adaptive system. Concurrent with the development of the maximum performance design, The Aerospace Corporation has performed similar work to produce a cost-effective system that would incorporate as many of the maximum design features as possible in conjunction with significant cost reductions. This design was aimed at bringing projected manufac-

turing costs down to the desired goal of \$200 to \$300 per consumer, with a minimum sacrifice of performance and reliability. Details of this design are described in Section III-C.

B. Maximum Performance Design

In the spring of 1975, GTE/Sylvania Incorporated was awarded a contract to develop a burglar alarm system that would meet the design approach described in Section III-A. The system was called the Maximum Performance Design (Fig. 3) because it was to incorporate as many as the general design concepts as possible with the single exception of the low-cost requirement.

The resulting system consisted of six subsystems:

- Central Processor
- Entrance Control
- Local Alarm
- Sensor Transmitters
- External Interface
- Central Station Module

1. The central processor. The central processor (Figs. 4 and 5) is the brain of the burglar alarm system. It continuously monitors all radio frequency traffic on the ac powerline and processes incoming alarm messages. It can support two-way communication with up to four entrance control units. It contains the logic for sounding an alarm; in case of multiple alarms, it establishes a priority. It has the capability of handling up to 16 sensor input devices. (The delivered prototype systems contain only four sensors



Figure 3. Overall Concept, Maximum Performance Design

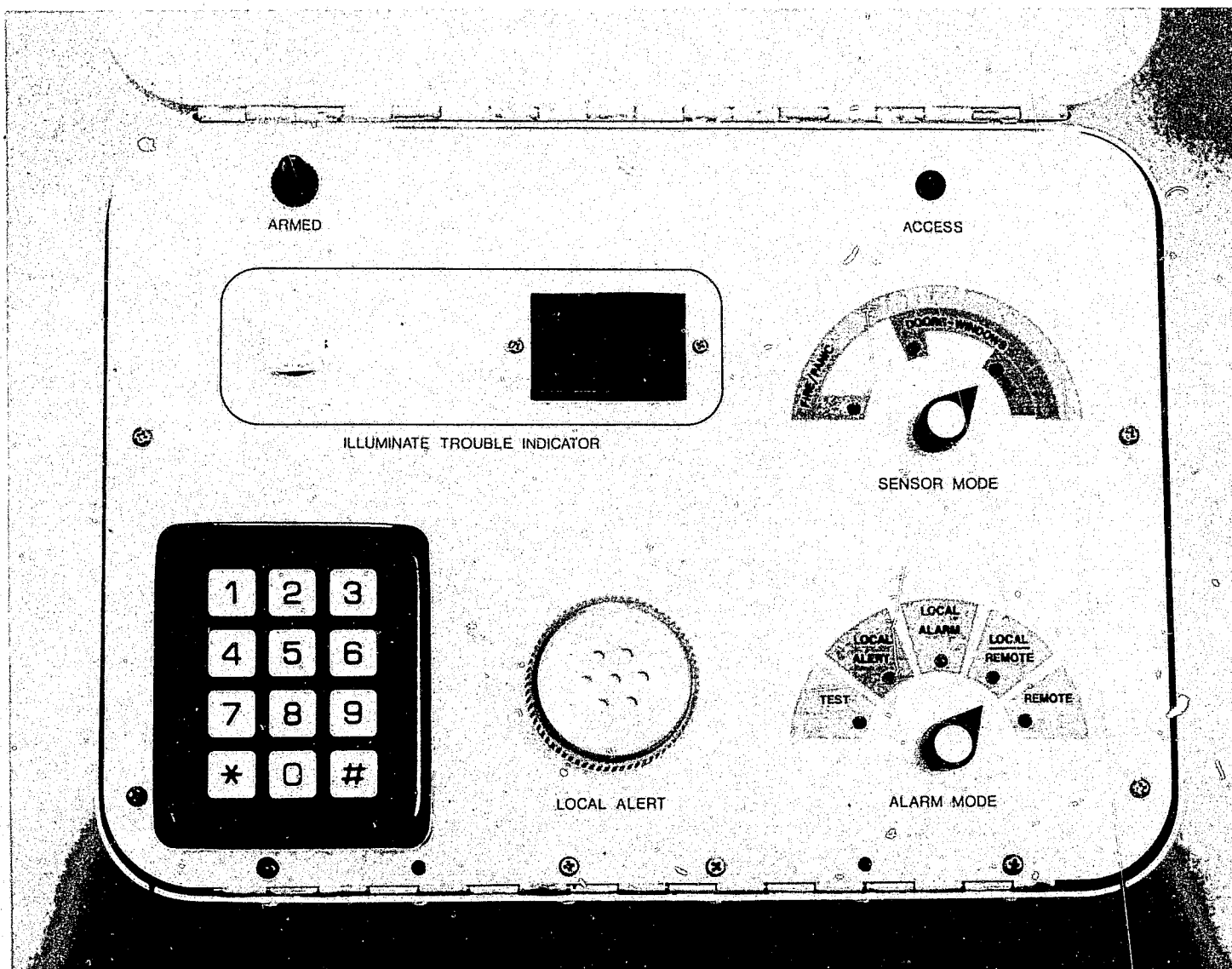


Figure 4. Burglar Alarm System Control Processor, Front Panel

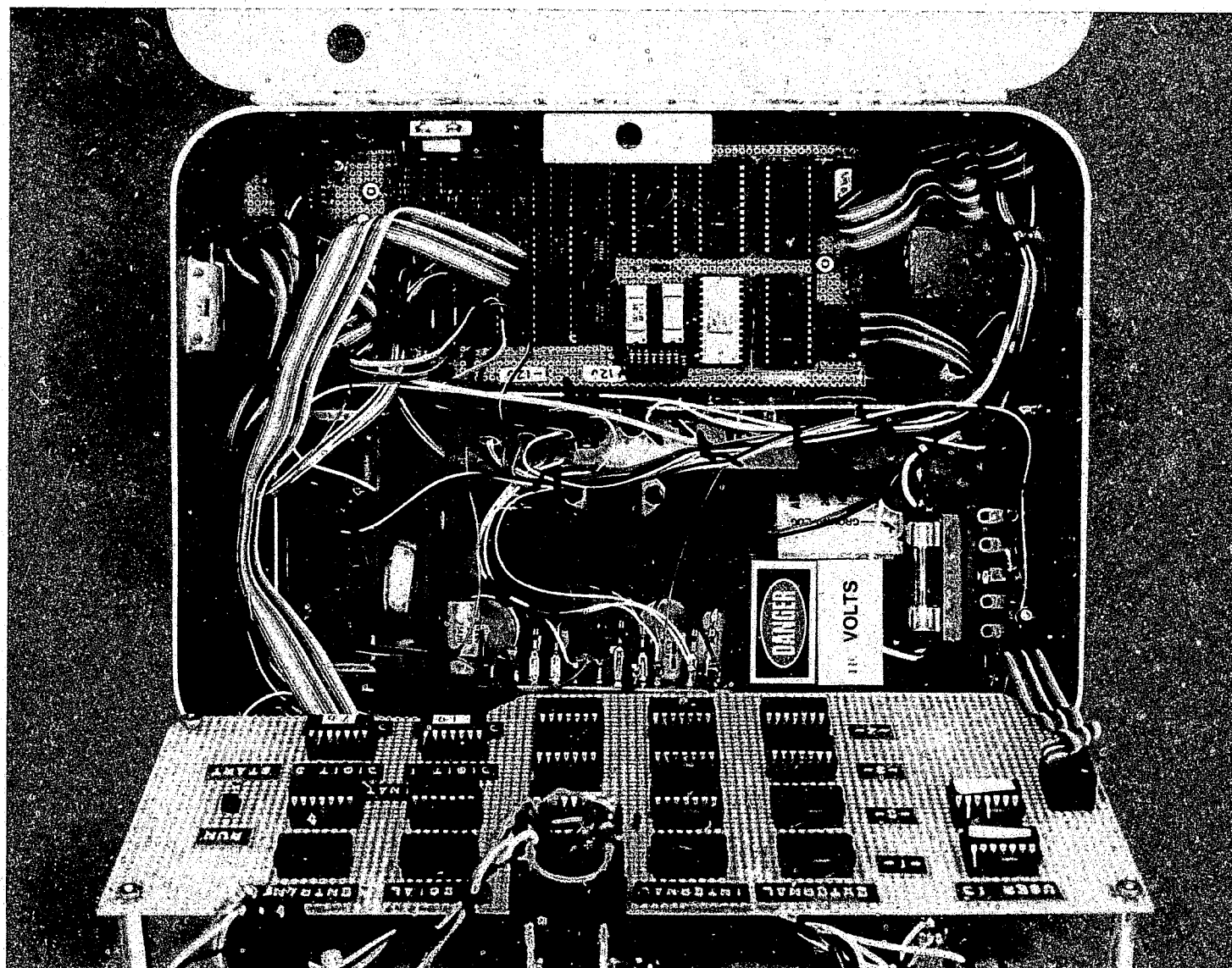


Figure 5. Internal View of the Central Processor

and a panic button.) Once initiated, the processor can be in two possible states — armed and disarmed, as follows:

<u>State</u>	<u>Operative functions</u>
Armed	Intrusion detection
	Fire alarm
	Status
	Panic
	Tamper
Disarmed	Fire alarm
	Status
	Panic
	Tamper

A local alert (Fig. 4) is provided on the processor. It is a sounding device to alert the occupant to some event of interest, but it is not a loud warning. The processor also alerts the user to any trouble in the system and displays the identity of the source of trouble on the trouble indicator (Fig. 4).

The processor activates a loud local-alarm bell (Fig. 6) that is received by a central monitoring station via the external interface module and leased telephone line.

2. Sensor-transmitters. The central processor receives most of its input data as digital signals transmitted over powerlines within the premises. Outlying intrusion sensors are connected via two wires to a sensor-transmitter (Fig. 7) plugged into a wall socket. Each sensor-transmitter has its own identification given to it by an inserted code plug. This allows the central processor to keep status and alarm/secure information on each sensor location and permits the user to change the operating modes of the system as needed. The sensor-transmitters send periodic status messages to the central processor. If the processor misses two consecutive status messages

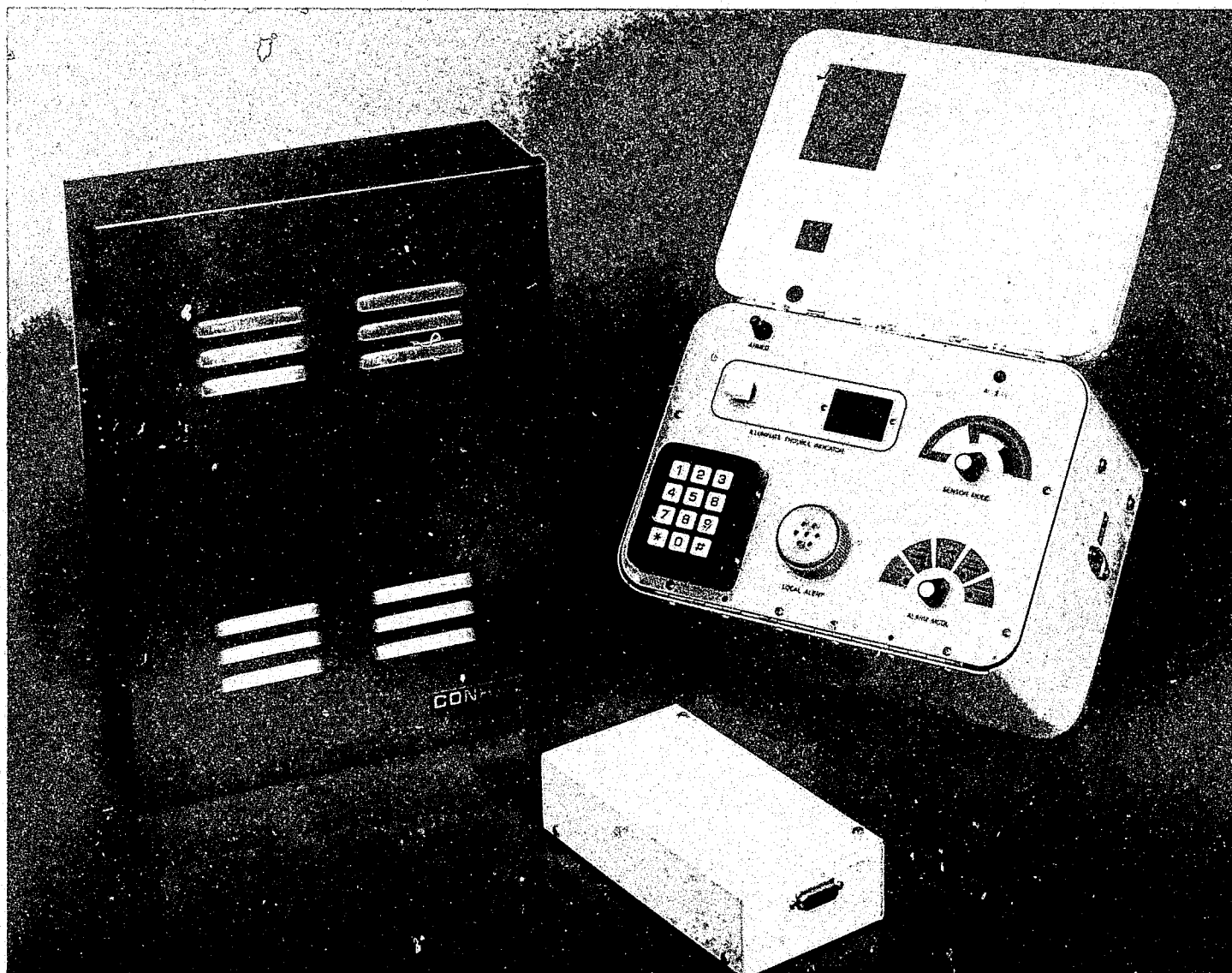


Figure 6. Local Alarm, External Interface and Central Processor

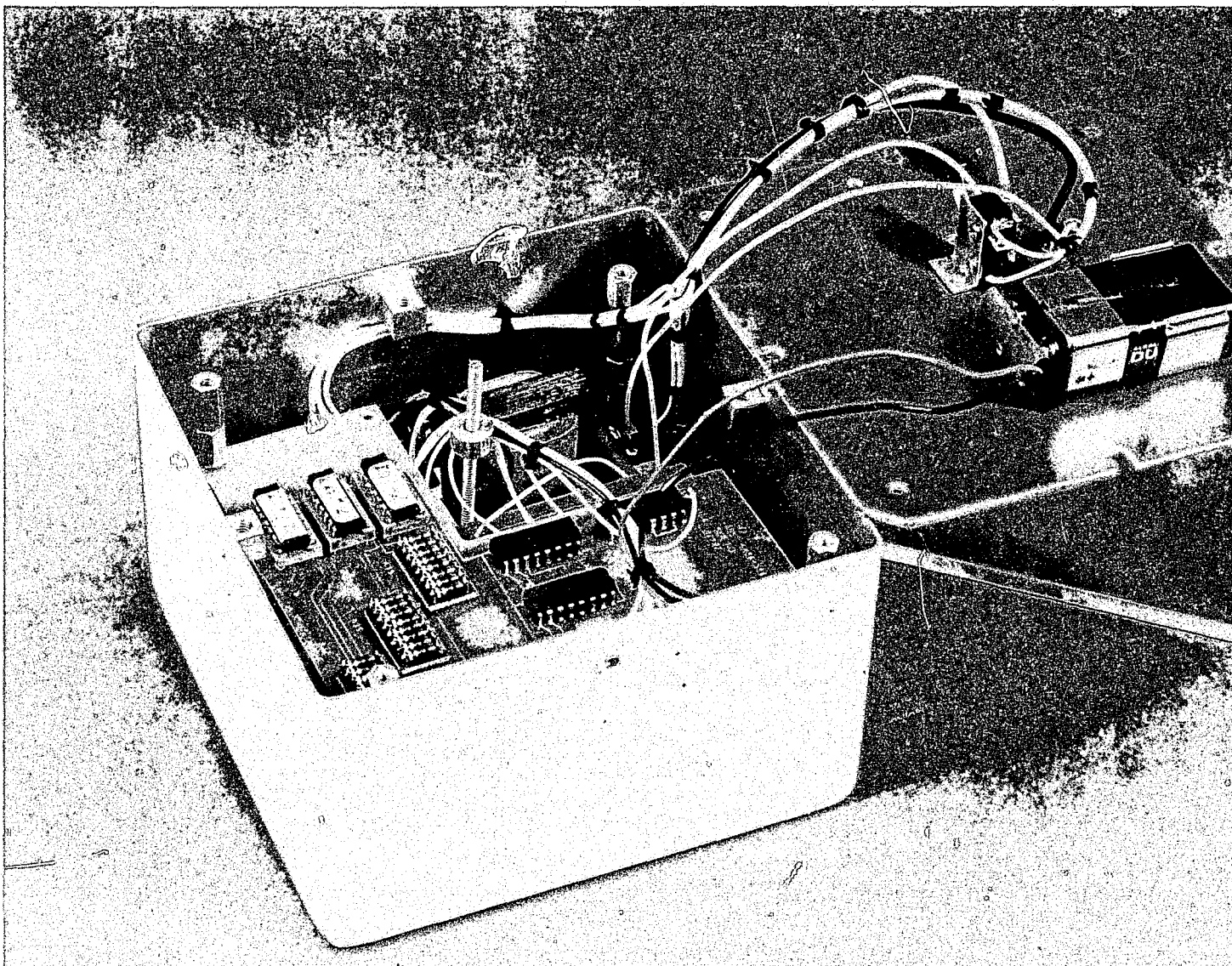


Figure 7. Sensor-Transmitter

from a sensor-transmitter, a trouble condition is flagged, and the user is notified by the trouble indicator the next time the system is armed or disarmed. The time between status messages is 1 hour, and these messages serve also as a monitor on the integrity of the powerline communication from sensors to processor. A blinking light notifies the user of trouble whenever the system is armed or disarmed. The source of trouble can be read on the processor's display panel (Fig. 4).

3. Sensor mode switch. By means of a sensor mode switch (Fig. 4), the user can set the processor to respond to any of the following three alarm classes:

- 1 Fire, tamper, panic, special
- 2 Fire, tamper, panic, special, perimeter
- 3 Fire, tamper, panic, special, perimeter, internal

4. Alarm mode switch. Similarly, by means of an alarm mode switch (Fig. 4), the user can set the processor to announce alarms in the following five ways:

- 1 Test
- 2 Local alert
- 3 Local alarm
- 4 Local alarm and external interface
- 5 External interface

When the sensor-transmitters are installed, individual code plugs are taken from the central processor (Fig. 8) and installed in each sensor-transmitter. The code plug defines the type of sensor (perimeter for doors and windows; internal, with switch mats or volumetric sensors such as infrared or ultrasonic; and fire/smoke detectors) and gives each sensor a unique numerical indication. The type identification allows the user to operate the system in a variety of sensor mode configurations. For instance, if

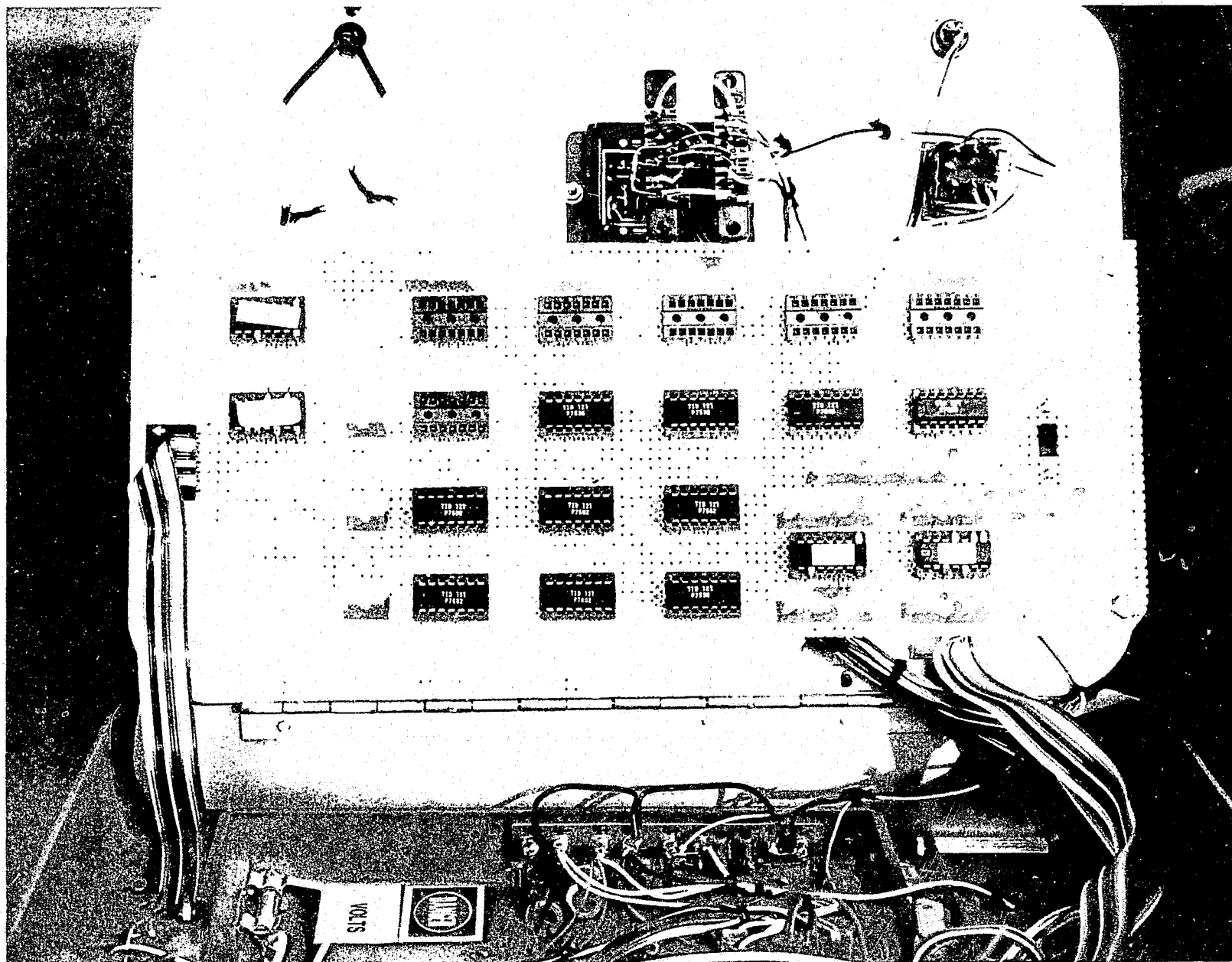


Figure 8. Central Processor Code Plug Board

the user wishes to leave a pet in the house during his absence, it would be desirable to ignore all internally generated alarms that may be activated by the pet.

5. User-control procedures. The sensor mode switch on the central processor (Fig. 4) has three positions that allow the system to monitor on the following three levels:

- 1 First position — fire, tamper, and panic alarms
- 2 Second position — all previous positions, plus perimeter sensors
- 3 Third position — all previous positions, plus internal sensors.

Taking the example of leaving a pet in the house, the user would set the sensor mode switch on the second position, allowing the emergency alarms to activate, protecting the premises with the perimeter sensors (doors and windows), but leaving the internal sensors dormant so they would not be activated by the pet as a false alarm.

The user may also select the alarm response mode desired, by using the five-position alarm mode switch (Fig. 4), with the following options:

<u>Position</u>	<u>Function</u>
1	Test — Sounds a noise and lights a light at the central processor
2	Local alert — Sounds a noise internally throughout the house
3	Local alarm — Sounds a loud noise outdoors
4	Local/remote alarm — The same as 3, but also a silent alarm to the central station
5	Remote — Only a silent alarm

6. Protective measures. The sensor mode and alarm mode switches give flexibility to the system, allowing the user to adapt its capabilities to a

variety of situations and uses. This versatility, however, needs protection from deliberate or inadvertent changes from the selected settings. The system, therefore, is designed with a keyboard (Fig. 4) on the central processor that allows access to the controls by authorized users only, through punching a four-digit combination code on the keys. When this is done, the processor goes into an access mode for a timed period of 1 minute. The access mode disarms the system automatically and allows the user access to the inside of the processor to change the combination, obtain code plugs, or change settings on the sensor mode and alarm mode switches. To further preclude false alarms, the processor will not allow the system to be armed at the processor front panel if the alarm mode switch (Fig. 9) is set in any of the external positions (positions 3, 4, or 5).

When trouble occurs during the user's absence, he is informed on his return by a flashing light at the keyboard. If an alarm has occurred during his absence, the user is informed by a flashing of the light emitting diode (LED) display (Fig. 4), with an identification of the alarmed sensor.

The entrance control unit (Fig. 9) is for the prevention of false alarms. The unit contains an electric door strike, a microprocessor, an arming switch, a door sensor switch, a tamper switch, two "panic" pushbuttons, and a powerline transmitter and receiver. The panic button arrangement is dual and requires two separate pressures to activate the system in order to eliminate false alarms by accidental pressure on a single button. When properly activated, the panic system rings the local alarm bell and simultaneously alerts the central station for police or guard force response.

The entrance control unit functions as an extension of the processor and its door-monitoring unit, which uses a keyboard as a door control unit during exit and reentry. The device consists of a 12-digit keyboard located on the external doorjamb and an electric strike with electronic surface mounted on

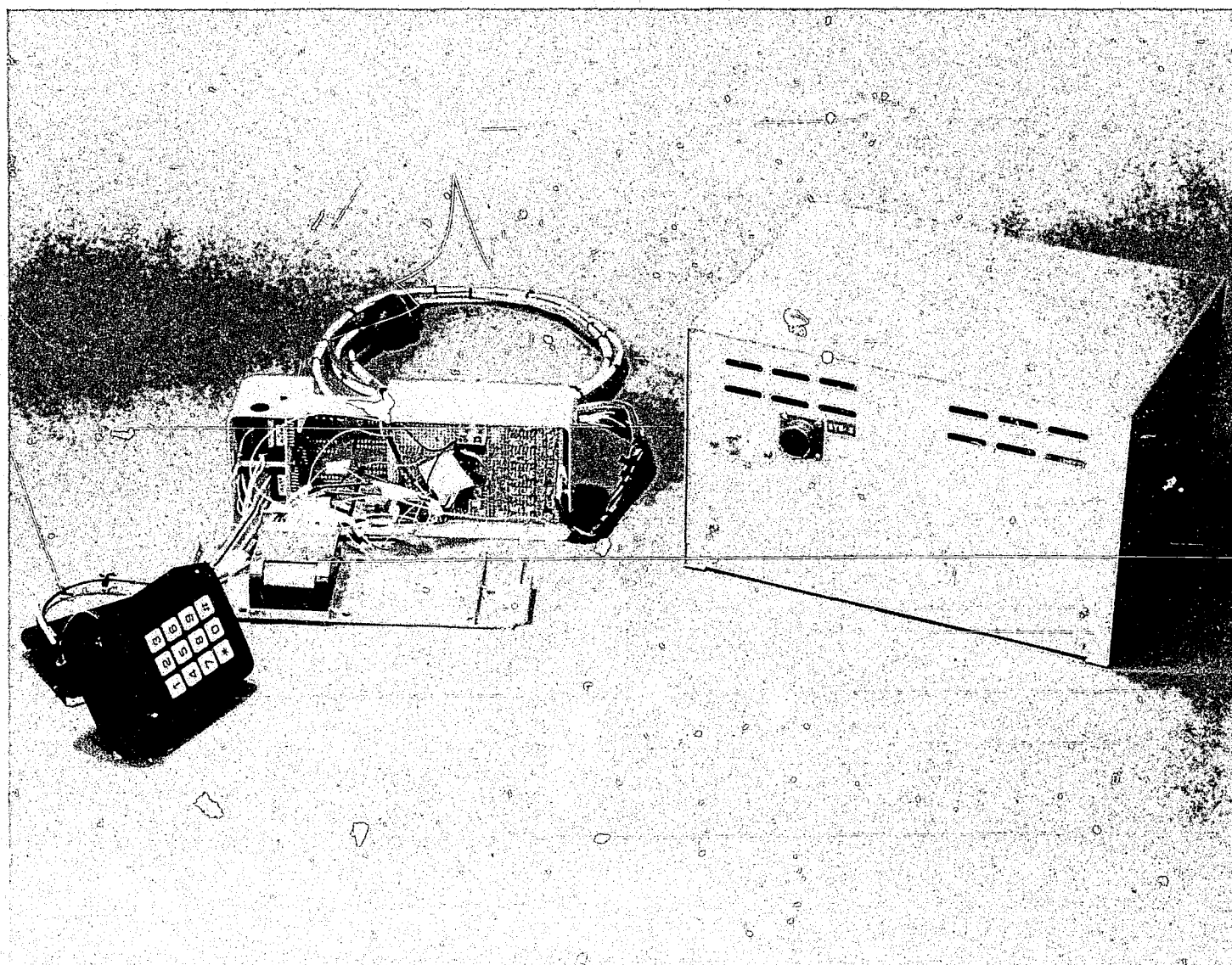


Figure 9. Entrance Control Hardware

the internal doorjamb. A surface-mounted, spring-loaded bolt assembly is then mounted on the inside surface of the door to mate with the electric strike. The 4-digit combination, which is set at the central processor, is used to disarm the system and gain physical access to the residence.

It is, therefore, impossible to gain authorized access to the residence without disarming the system. Since the keyboard combination is transmitted over powerlines to which unauthorized persons may have access, internal provisions have been made for the system to further encode these data. This precludes a potential intruder from simply recording and playing back the data at the appropriate times. Colocated at the entrance control are a keyboard tamper switch, panic buttons, a door sensor switch, and a recessed system arming button. When exiting the residence all that is necessary to arm the system is to press the arming button and close the door.

7. Alarm and reporting system. The local alarm (Fig. 6) is the primary audio device in the system. Its primary power is supplied by a hardwired link to the processor. With the optional battery module, it will sound for 5 minutes at full volume if the link to the processor should be cut.

The sensor transmitter unit is a general purpose device that is compatible with the different types of sensors used in the system. In the event of a change in sensor state, the transmitter will transmit either an alarm or a secure message at the rate of 1 per minute for 5 minutes. There will also be an alarm message generated if any attempt is made to physically disconnect the sensor transmitter from the ac outlet that it is plugged into.

Fire, panic, tamper, and intrusion messages cause a 5-minute alarm. The panic feature allows the user to activate the door alarm on command. The tamper feature automatically activates the alarm system if the outside keyboard is removed, or the outside bell box is opened or removed. Intrusion alarms are announced only when the system is armed. Fire alarms are given priority over intrusion alarms by the processor.

Provision has been made for one additional type of alarm message as a special alarm. This is initiated by a special transmitter on command from any user-supplied sensor that is elected.

The several alarm outputs are shown in Table 1.

The external interface, an optional module for the user, allows the alarm system processor to be interfaced with a dedicated telephone line, as part of a communication network of approximately 25 users monitored by the central alarm station module. There are two modes of communication that the external interface will support: polled and nonpolled. In the polled mode, the central station sends an inquiry message to each individual alarm processor which responds by sending an alarm status message back to the central station. A nonpolled message is one that the alarm system processor self-initiates whenever an alarm occurs, without a prior inquiry message from the central station. The external interface unit consists of a 600-bit per second transit-receive modulator-demodulator for synchronous operation on a half-duplex voice-grade telephone channel. The dc power for the unit will be furnished by the processor. The central station module will provide the communications, data processing, and display equipment needed to monitor the individual alarm installations from a central station using dedicated telephone lines.

Generally, a number of subscribers will share a single phone line; therefore, an address will be included in this message. That address will be the same as the one used for powerline carrier communications within the burglar alarm system. It will be the 16-bit address contained in each system's identification code. All the alarm systems that share a common line

Table 1. Burglar Alarm System — Alarm Outputs

Item	Fire	Panic	Intrusion	Tamper	Special
Test	20-second test light and local alert	20-second test light and local alert	20-second test light and local alert	20-second test light and local alert	20-second test light and local alert
Local Alert	5-minute pulsating local alert and bell alarm	5-minute steady bell alarm	5-second local alert	5-minute steady bell alarm	5-minute local alert
Local Alarm	5-minute pulsating local alert and bell alarm	5-minute steady bell alarm	5-minute steady bell alarm	5-minute steady bell alarm	5-minute local alert
Local Remote	5-minute pulsating local alert and bell alarm with modem transmission	5-minute steady bell alarm with modem transmission	5-minute steady bell alarm with modem transmission	5-minute steady bell alarm with modem transmission	5-minute local alert with modem transmission
Remote	5-minute pulsating local alert and bell alarm with modem transmission	5-minute steady bell alarm with modem transmission	Modem transmission only	5-minute steady bell alarm with modem transmission	5-minute local alert with modem transmission

will receive the interrogations that are addressed to any one of the systems on that line. However, only one system code will match and recognize the particular address code and respond to the interrogation. The interrogated system will respond with a message that contains its address and a series of bits to show which (if any) alarms are present. In the direct mode (or non-pollled) operation, the central station remains passive, and alarm messages are sent by the subscribers if and when an alarm is generated. The format of the alarm messages is identical to the format used to respond to an interrogation in the polled mode, and the action of the central station module is the same.

C. Low-Cost Adaptive System

The second system was developed by The Aerospace Corporation in concert with various subcontractors. The same overall design requirements used in the development of the maximum performance design were applied to the low-cost adaptive system, with special attention given to the goal of a low-cost, produceable burglar alarm. The purpose was to incorporate as many of the desirable features of the maximum performance system as possible, with significant cost reductions in the subsystems to obtain the objective of a modest consumer price. As a result, the effort was directed toward commercially practical hardware components that could be applied to an overall system design. Four specific hardware developments evolved: (1) a reliable, low-cost intrusion detector; (2) a miniature radio receiver and transmitter; (3) a low-cost microcomputer controller; and (4) a deadbolt entrance control unit. As applied to system requirements, these items contributed a higher reliability and a lower overall cost to any system compatible with the basic design approach. The four hardware items could be applied to the several functional areas of any total system package (see Fig. 10).

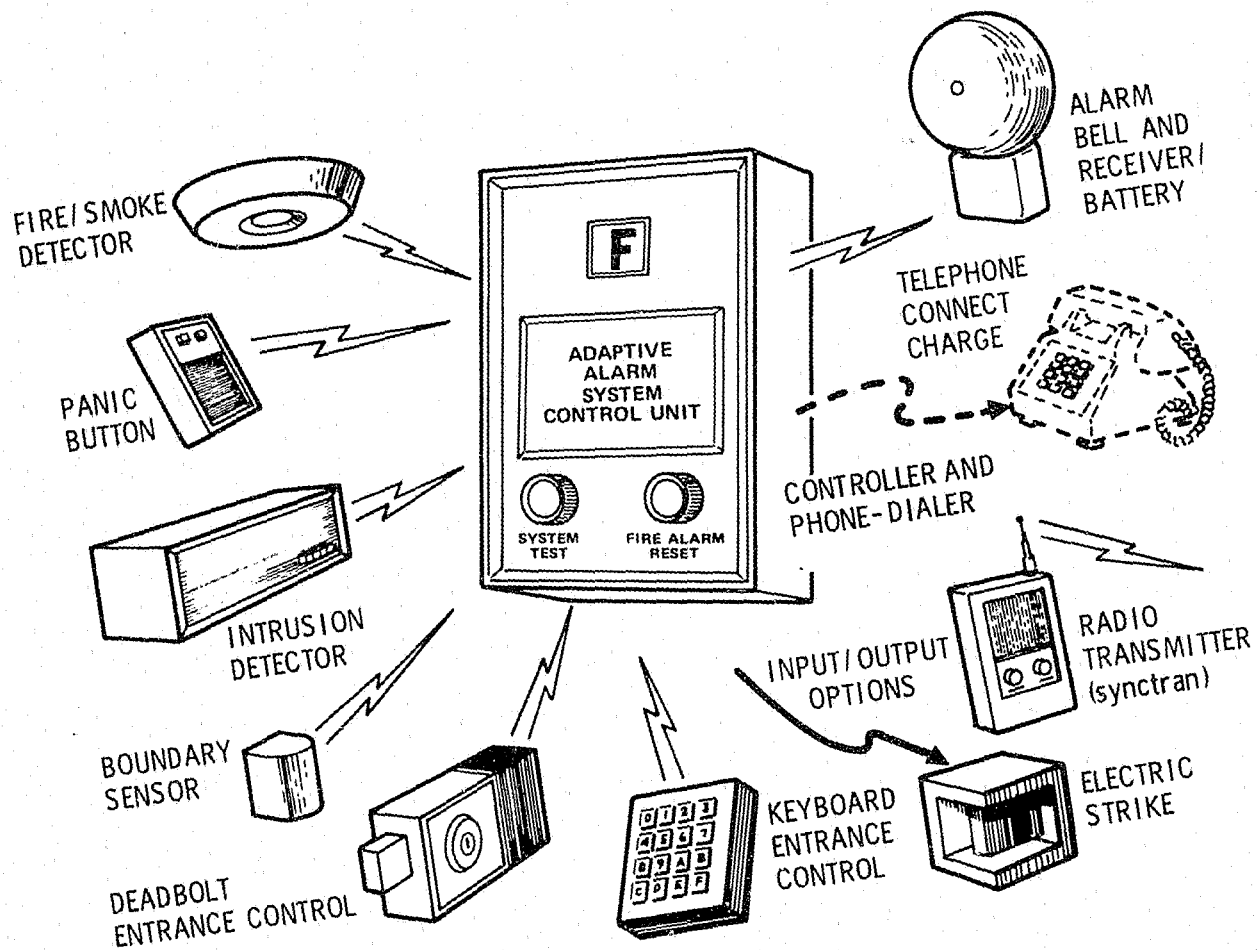


Figure 10. Total System Package

1. Intracommunications. The low-cost adaptive system was developed as a wireless burglar alarm system. Miniature radio sender modules were used to transmit coded signals to a radio receiver internal to the protected area. These radio modules could be located at doors and windows and operated with internal sensors, such as floor switch mats, ultrasonic, infrared, or fire and smoke detectors. This allows both boundary protection of the shell of the premises and intrusion protection within the premises. A controller (Fig. 10) would use a radio receiver and microprocessor to detect the radio module messages and perform the logic for correct warning or alarm. The advantages of this system, in comparison with the maximum performance design (Section III-B) were the mobility of the controller, whose sensor transmitters needed no plug-in and was not dependent on fixed communication lines, and the low cost of installation.

The controller would activate the alarm system by radio or landline message, using computer logic to safeguard against false alarms and human error. Legitimate entrance would be allowed by key control disarming. Although the original microcomputer controller design concentrated on its application to a local premises burglar alarm system, the capacity for additional features without materially increasing the cost was apparent early and became a consideration for follow-on developments. Keyboard coding for control, telephone connections, radio communication to a central station, automatic door-locking, monitoring of electric appliances, and automatic lighting controls are options available within existing technology (see Fig. 11). A discussion of a follow-on microprocessor that would incorporate these features is provided in Chapter V.

The radio communication system was called a "near-field" transmission system because it used coded low frequencies (0.15 to 10.0 MHz), and the distances over which the system would transmit would be less than one-third

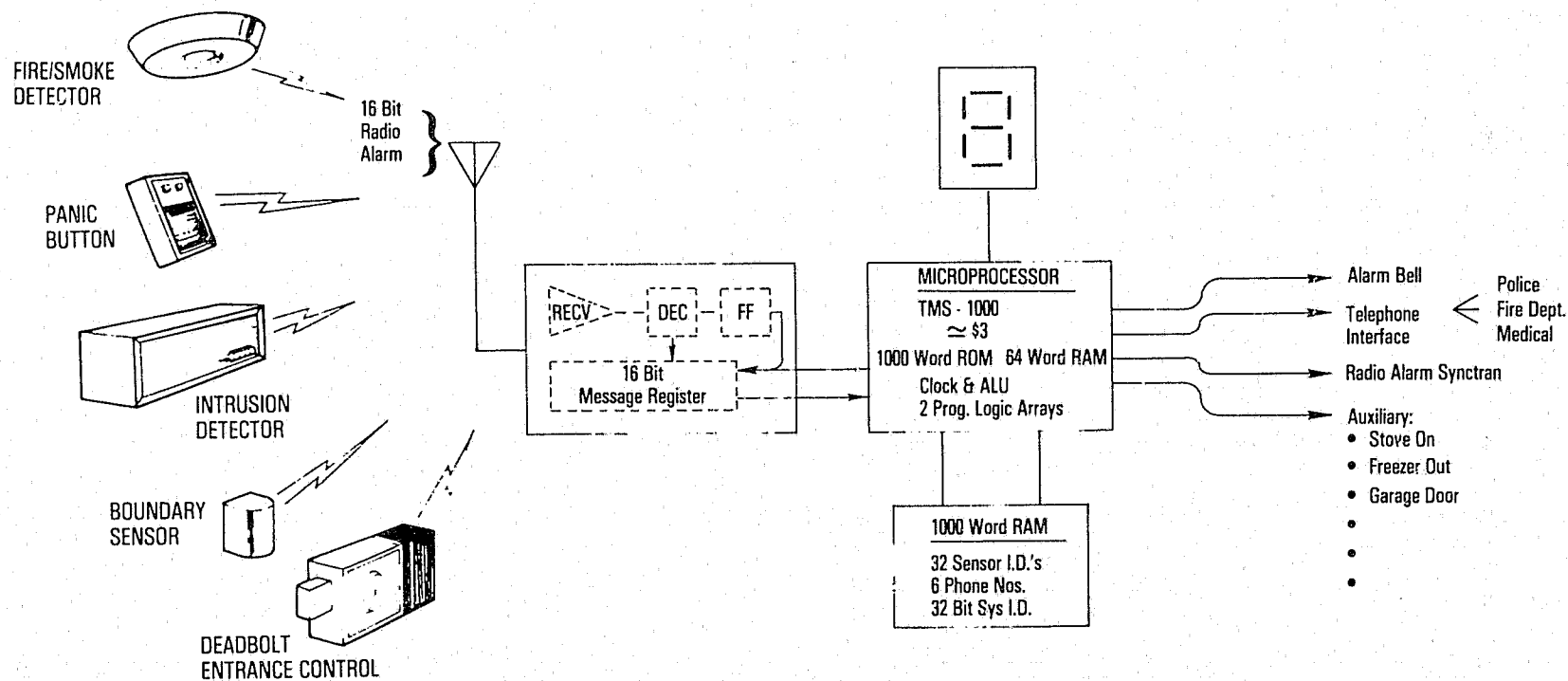


Figure 11. Adaptive Alarm System

wavelength. The field intensity of the transmitted signal drops off rapidly with distance from the transmitter. Performance requirements were for detection of the sender unit at about 30 feet, but less than 80 feet, with a probability of 99 percent. The purpose of this requirement was to allow multiple use of the system in high-density business and residential areas.

2. Sensors. The near-field radio communication system uses a sensor-transmitter (Fig. 12) that transmits a 16-bit coded digital signal. Fifteen of these bits represent the assigned identification code of the sensor; the sixteenth bit gives its status: "zero" for an unsecure condition; "one" for a secure state.

Each radio sender module transmits a unique 15-bit permanent identification code as a binary sequence, and the controller provides a means to read-in the identification code of each of the sender modules associated with it. Subsequently, the triggering of any of these radio sender modules will be detected by any alarm receiver lying within a distance of 40 to 50 feet from the sender, but only the controller microprocessor that is programmed for this particular sender will register this transmission. Utilizing this 15-bit code, there will exist at least 32,000 sender code combinations; consequently, the probability of more than one controller/receiver responding to any specific radio sender module will be negligible.

a. Boundary sensors. The shell of the protected premises is guarded by boundary sensors (Fig. 13) using magnetic reed switches. These boundary sensors are placed at possible points of entrance, such as doors and windows. When the system is armed, opening any of these entrances, or tampering with any of the sensors, will activate a signal to the controller through its miniature radio sender module. Battery powered, with a 10-year life, and purchasable at an estimated production cost of \$10, these sensors can be used in the number needed to provide security to all entrances.

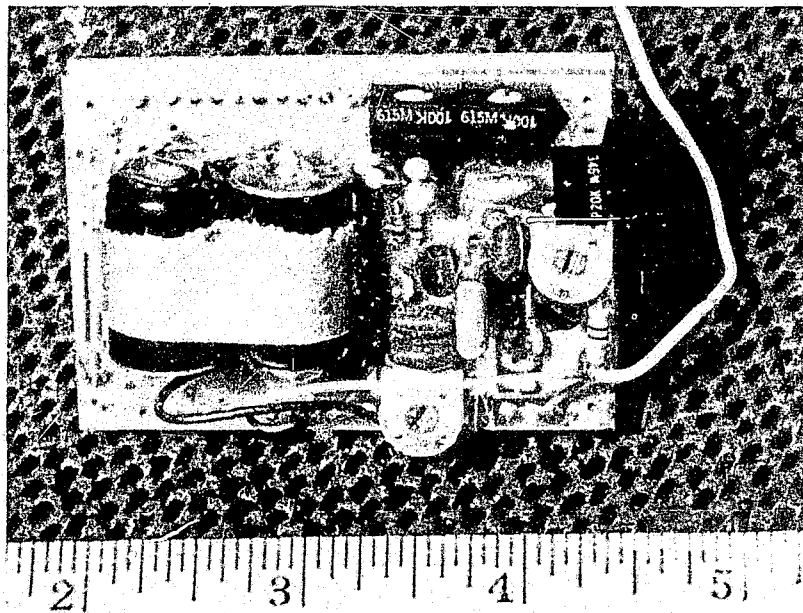
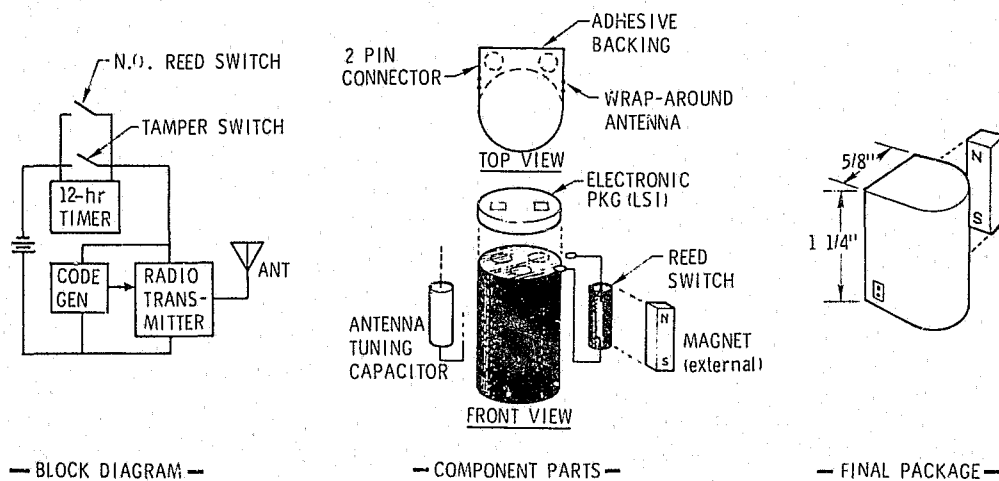


Figure 12. "Brassboard" or Developmental Sensor-Transmitter



GOALS

- 10-YEAR LIFE
- \$10 USER COST
- 35,000 OPERATING CYCLES
- NONREUSABLE PACKAGE
- TAMPER PROOF

Figure 13. Boundary Sensor

b. Intrusion sensors. The interior of the premises can be guarded by thermal intrusion devices that detect moving thermal energy sources by infrared emanations. As with the boundary sensors, these devices are battery powered, with a life of 5 years; they have an estimated production cost of \$60. Coded messages are transmitted to the controller via miniature radio sender.

The intrusion sensor adopted for the prototype system is an improved model (Figs. 14 and 15) developed by the Rossin Corporation, and it incorporates a two-beam mirror arrangement and faster response circuitry to detect fast-moving targets. This equipment is described in detail in Chapter IV.

c. Fire/smoke detectors. The system provides for fire/smoke detectors that sound an audio alarm via the controller on danger conditions.

3. Controller. The heart of the system is a controller that communicates with the sensors and other control inputs, logically determines the alarm condition, and executes the alarm announcements. The controller consists of a microprocessor circuit board, a user control panel for command of the system, and a near-field radio communication receiver printed circuit board. The controller responds to inputs through a prescribed logic sequence and generates output signals through its own circuitry.

a. Microprocessor. The microprocessor in the first system uses a Pro-Log Corporation one-card system. Specifications and features of this prototype development microprocessor are shown in Figures 16 and 17. The microprocessor will accommodate 16 sensors in a single system, 1024 words of read-only memory, and 64 words (320 characters) of random-access memory. It contains a clock, a program counter, an accumulator, several housekeeping registers, and output latches for addressing purposes and off-board digital display.

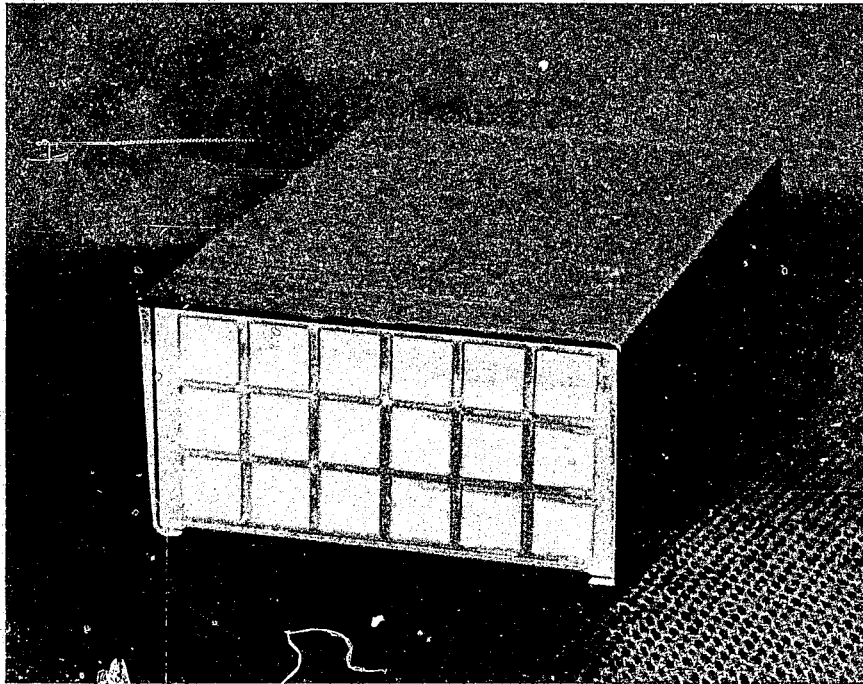


Figure 14. Rossin Infrared Sensor in Operation

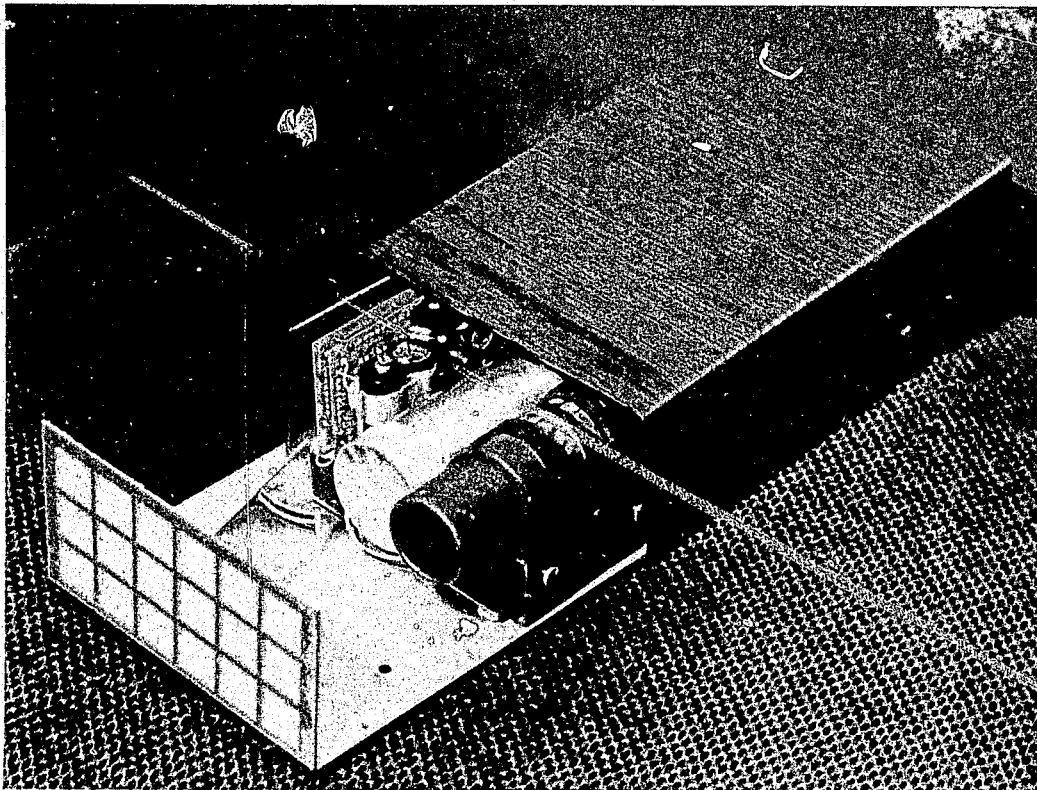


Figure 15. Rossin Infrared Sensor with Chassis
Partly Removed from Case

Card Dimensions

4.5 inches high
6.5 inches long
0.48 inch maximum profile thickness
0.062 inch printed circuit board thickness

Includes

Card ejector
One 4004 CPU
One 4002 RAM and four RAM sockets
One 1702A ROM and four ROM sockets
Master power-on and external reset circuit
Crystal clock circuit
Four TTL output ports (16 lines)
Four TTL input ports (16 lines)
One MOS output port (4 lines)
CPU test input (MOS)

Maximum Systems Capabilities

Four 4002 RAMs (320 four bit characters)
Four 1302, 1602, or 1702 ROMs (1024 words of program memory)
20 output lines

16 TTL port lines
4 MOS RAM port lines

16 TTL input lines

Instruction Execution Capability

Capable of executing all 46 of the 4004 CPU instruction except for DCL and WPM
11.2 microseconds instruction execution time

Logic Levels Of External Connections

Low level active:

TTL Port: TTL compatibility and loading
MOS Input: TTL compatibility
MOS Output: Drive capability, one LPTTL or one TTL load with 12K pull-down to -VDD

Power Requirements

+VCC = +5 volts 5% @ 550 mA maximum fully loaded (30 mA per RAM, 35 mA per ROM)
GND = 0 volts
-VDD = -10 volts 5% @ 350 mA maximum fully loaded (30 mA per RAM, 35 mA per ROM)

Connector Requirements

56 pin, 28 position dual-readout on 0.125 centers

EDGE CONNECTOR PIN LIST									
PIN NUMBER					PIN NUMBER				
SIGNAL FLOW					SIGNAL FLOW				
SIGNAL					SIGNAL				
+5 VOLTS	IN	2	1	IN	+5 VOLTS				
GROUND	IN	4	3	IN	GROUND				
-10 VOLTS	IN	6	5	IN	-10 VOLTS				
RD-8*	OUT	8	7	OUT	OUT 2-8*				
RD-4*	OUT	10	9	OUT	OUT 2-2*				
RD-2*	OUT	12	11	OUT	OUT 2-1*				
RD-1*	OUT	14	13	OUT	OUT 2-4*				
CLOCK 01*	OUT	16	15	OUT	OUT 1-8*				
TEST*	IN	18	17	OUT	OUT 1-2*				
OUT 3-8*	OUT	20	19	OUT	OUT 1-1*				
OUT 3-2*	OUT	22	21	OUT	OUT 1-4*				
OUT 3-1*	OUT	24	23	OUT	OUT 0-8*				
OUT 3-4*	OUT	26	25	OUT	OUT 0-2*				
RST*	OUT	28	27	OUT	OUT 0-1*				
EXT RESET*	IN	30	29	OUT	OUT 0-4*				
IN 0-1*	IN	32	31	IN	IN 2-8*				
IN 2-1*	IN	34	33	IN	IN 0-8*				
IN 0-2*	IN	36	35	IN	IN 2-4*				
IN 2-2*	IN	38	37	IN	IN 0-4*				
IN 1-8*	IN	40	39						
IN 3-8*	IN	42	41						
IN 1-1*	IN	44	43						
IN 3-1*	IN	46	45						
IN 3-2*	IN	48	47						
IN 1-2*	IN	50	49						
IN 3-4*	IN	52	51						
IN 1-4*	IN	54	53						
CLOCK 02*	OUT	56	55						

Figure 16. Specifications of PLS-401 System

- Single card programmed logic system for prototypes or production
- 1024 words of ROM program memory capacity (4 ROMs)
- 320 characters of RAM register storage capacity (4 RAMs)
- Four output ports (16 lines)
- Four input ports (16 lines)
- One RAM output port (4 lines)

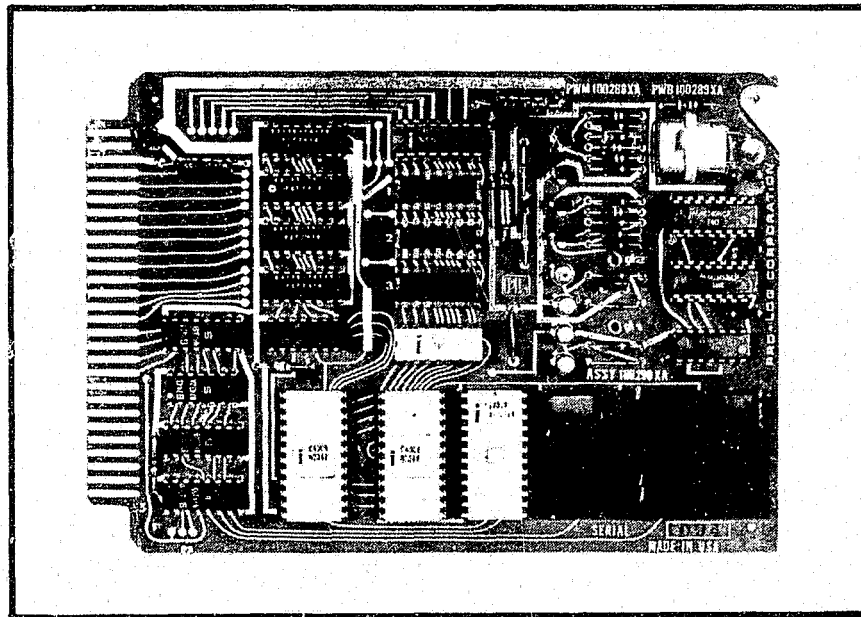
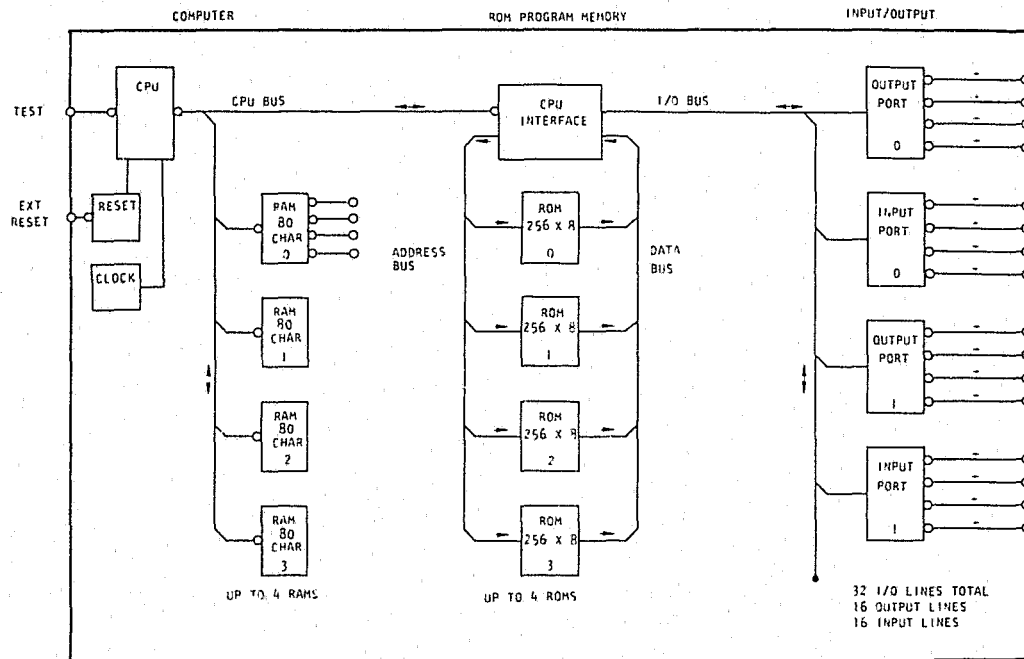


Figure 17. Features of PLS-401 System

b. User controls. Although the large-scale integrated (LSI) circuitry of the adaptive alarm system is highly sophisticated, the principal objectives were to simplify its operation for use by low- to moderate-income occupants of businesses and residences, and to circumvent false alarms by reducing the possibility of human error and building logic into the system.

The system is armed when the door is locked by the occupant and disarmed when the door is properly unlocked. The system itself distinguishes between inside and outside arming.

If any sensor is left open when arming, the system notifies the occupant by an audio alert signal. If the condition is not corrected, the system ignores the open sensor to prevent a subsequent false alarm.

The controller front panel (Fig. 18) has only three user controls: a test button, a fire alarm reset button, and a single character light emitting diode (LED).

- Test button — This allows the user to test the system. An unsecure condition, such as an open window, will be identified on the LED display for correction.
- Fire alarm reset button — This shuts off the fire alarm; it is intended for firemen who do not have a key to the burglar alarm system.
- LED display — This identifies each sensor by the channel number assigned by the user. Channel numbers may be assigned to sensors upon installation of the system and when new sensors are added.

c. Display panel. A seven-segment display (Fig. 18) is located on the controller housing to display information to the user. Through 32 distinct patterns (hex character and optional decimal point), the same number of separate sensors can be shown, indicating by the symbol which class is displayed (boundary, internal, fire, etc.). During an alarm, the display will

SEVEN-SEGMENT LED
DISPLAY PANEL

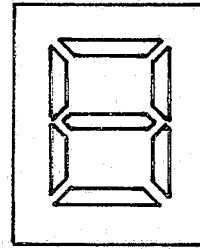


Figure 18. Controller, Front Panel

show the channel from which the signal came, if it is otherwise blank. On arming, the display will flash any open sensors for 20 seconds and accompany the visual warning with an audible alert to inform the user of an unsecure condition.

d. Receiver. Two pilot models of the receiver were developed, one by Hoffman Information Identification, Inc., and the other by Symtec, Inc.

The Hoffman receiver (Fig. 19) contains a superheterodyne front end that produces an intermediate frequency of 455 kHz. The automatic gain control level is monitored; if it is out of a preset range, an assumption is made that radio frequency interference exists and a signal is sent to the logic section to ignore incoming data. This eliminates false alarms from exterior sources and permits operation of the system in proximity with other occupied areas.

Detected audio is put into a phase-locked loop functioning as a frequency shift keying discriminator. The logic section operates on this discriminator to check the validity of data and collects the 16 bits (station identification signal and status) in a shift register. Simultaneously, a flip-flop is set to advise the microprocessor that a valid radio transmission has been received, and the data are stored.

In the Symtec receiver (Fig. 20), the input signal from a ferrite core antenna coil is fed to the input radio frequency (RF) stage, an amplifier that has a tuned circuit output transformer coupled to an amplifier-discriminator pack. The output level from this is a voltage level that shifts with input frequency. With no input, the level is about 5 volts; a 430-kHz input gives a voltage of about 3 volts; 400 kHz gives about 7 volts. The output signal is smoothed so that it responds to input frequency shifts at a maximum rate of about 500 Hz.

Figure 19. Hoffman Receiver Circuit Diagram

CONTINUED

1 OF 2

Figure 20. Symtec Receiver Circuit Diagram

Output from the Symtec receiver is compared with a preset level (interference level) in a comparator whose output is fed to one input of an exclusive "or" gate. The sense of the comparator is such that its output is low when a signal of 400 kHz is being received. A 400-kHz oscillator signal, switched on and off at about a 50-Hz rate, is fed to the other exclusive "or" input. When the oscillator is on, the receiver output will be low, making both inputs to the exclusive "or" low; when the oscillator is off, both inputs will be high. If the receiver is detecting the 400-kHz signal, the output from the oscillator will be low. This level is integrated, then compared with the interference delay level. The comparator output provides the interference signal level. If interference is present, the receiver will not detect the 400 kHz in the correct amplitude and phase; the exclusive "or" output will go high. If interference persists, the voltage will integrate up to trip the comparator and cause the interference signal line to go to zero.

4. Alarms. The system alarm bell rings steadily for burglary and emergency conditions and pulsates for fire alarms. All alarms ring for 15 minutes and may be stopped by disarming the system. In most cases, a 20-second warning precedes the alarm bell. The fire/smoke detector (Fig. 21) will trigger the alarm system on a danger condition. Both the alarm bell and the fire/smoke detector are connected to the controller position(s) by internal wiring.

5. Transmitter. Both the Hoffman (Fig. 22) and the Symtec (Fig. 23) companies have also produced transmitters for incorporation into the low-cost adaptive system.

Each transmitter sends a carrier any time a sensor is disturbed. The carrier contains a 16-bit data word: the first 15 bits identify the transmitter (sensor); the last bit is the sensor status. Logic "0" is equivalent to sensor reed switch open (undisturbed); Logic "1" indicates sensor reed switch

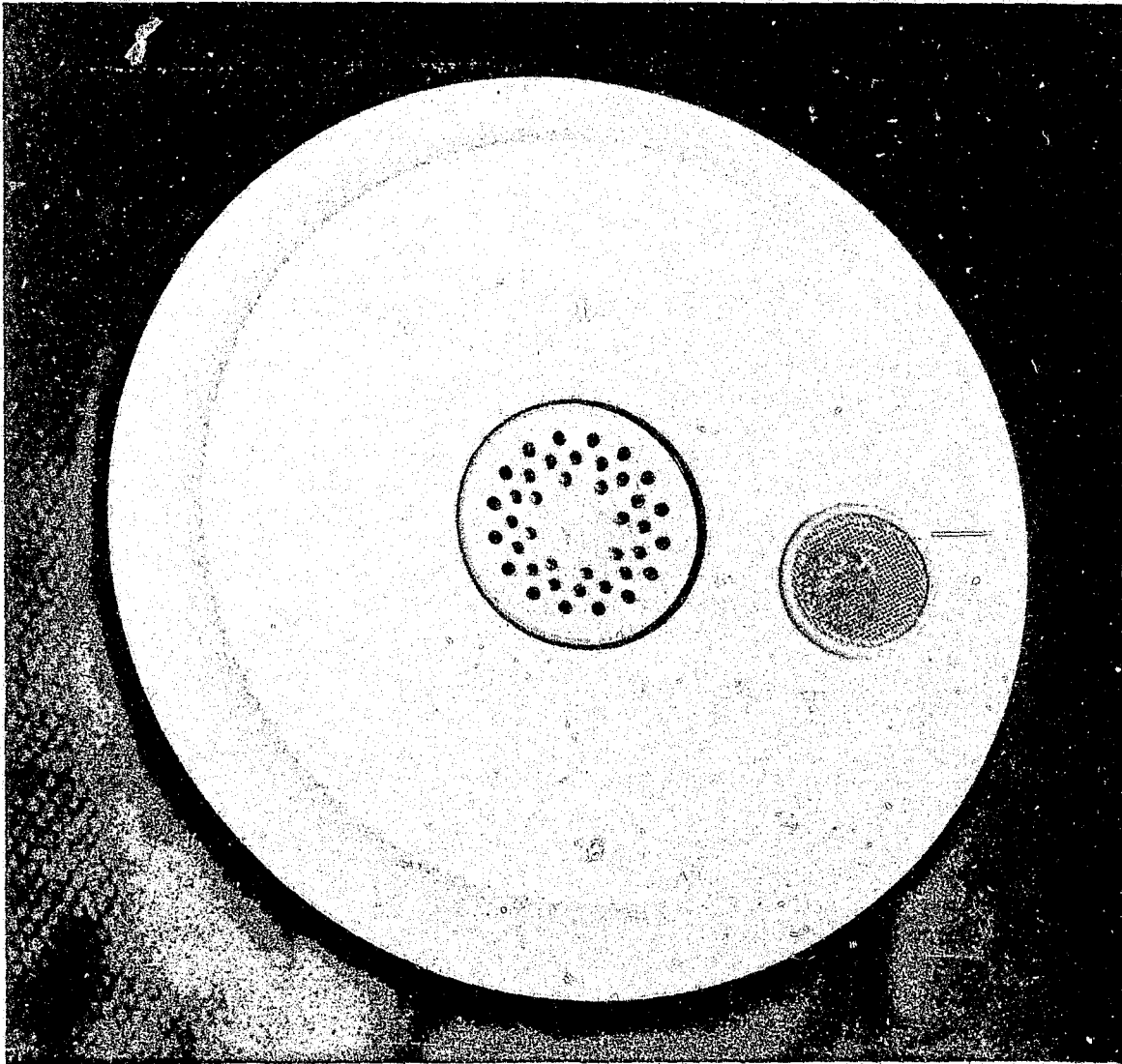


Figure 21. Fire/Smoke Detector

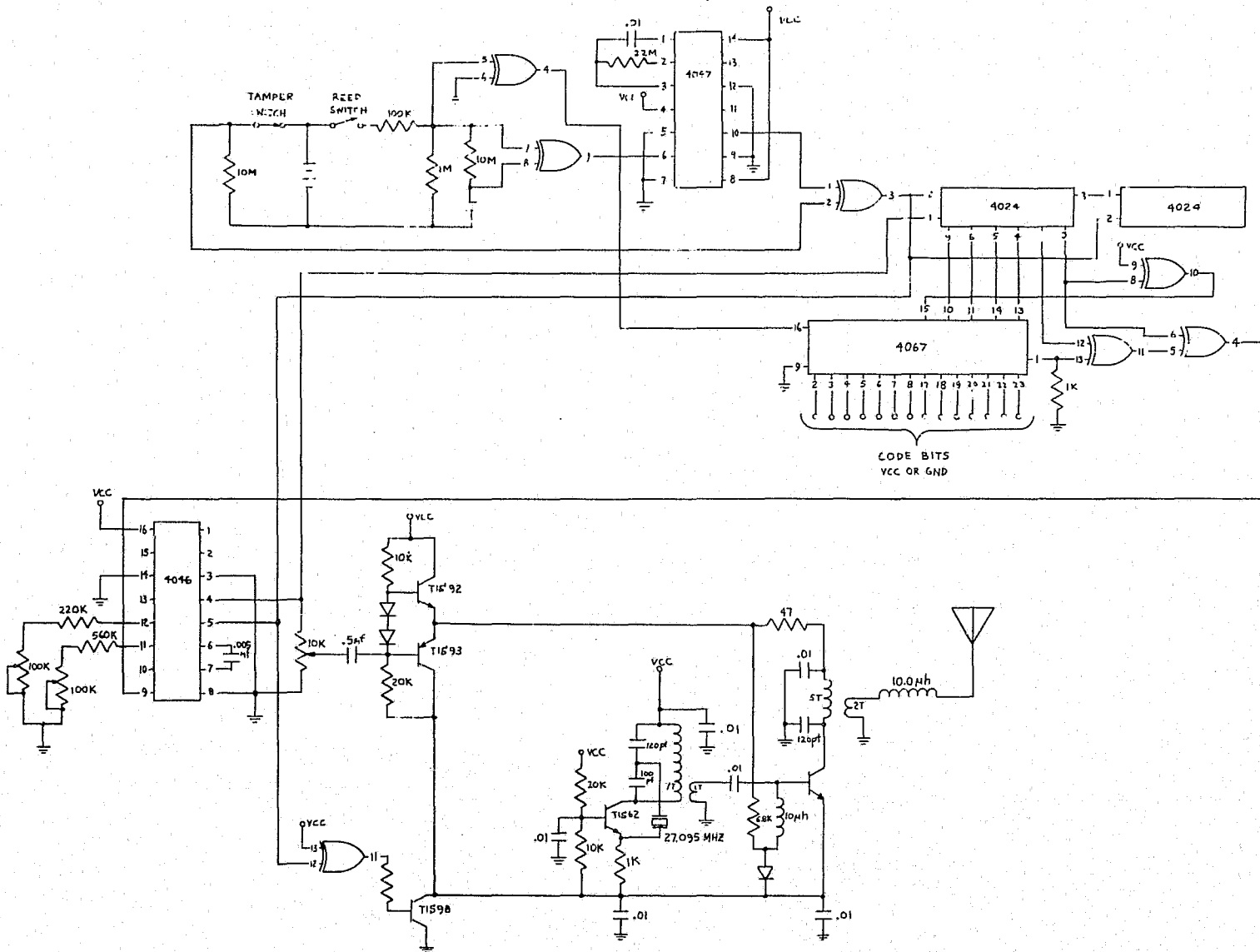
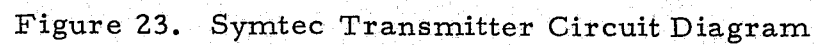


Figure 22. Hoffman Transmitter Circuit Diagram



closed (disturbed). The modulation technique is a combination of amplitude modulation and frequency shift keying.

6. Lock design. The fourth hardware item resulting from the Aerospace low-cost, adaptive alarm system concept was a single point user control from a deadbolt lock at the entrance to the premises.

To reduce the probability of user-caused false alarms, Aerospace determined that a single arm/disarm control should be used. The control should be situated conveniently as part of the user's normal living routine, and guarded against error by computer logic.

The preferred solution was a deadbolt lock at the main entrance, which would turn the alarm system on and off as the user left or entered the premises. This required a special lock, but for security reasons, it was desirable that the outward appearance not identify the lock as part of a burglar alarm system.

A subcontract was let to the National Lock and Hardware Co. in Rockville, Illinois, to develop such a lock device. It was required that the device closely resemble a commercial model made by the same company and marketed through the Sears Roebuck Co. chain. Modifications to the commercial model were to be simple and reliable and not add significantly to the end item cost. The subcontractor was successful in meeting these requirements and delivered 10 modified locks as specified by Aerospace (see Fig. 24). Limited on-off cycle testing has shown 100-percent operating reliability when combined with the electrical interface logic circuit designed by Aerospace.

With the special entrance lock installed, an occupant need only lock the door to arm the alarm system, or unlock it to disarm the system. If desired, a remote disarm switch may also be used. The logic system distinguishes inside arming (door locked from the inside) from outside arming.

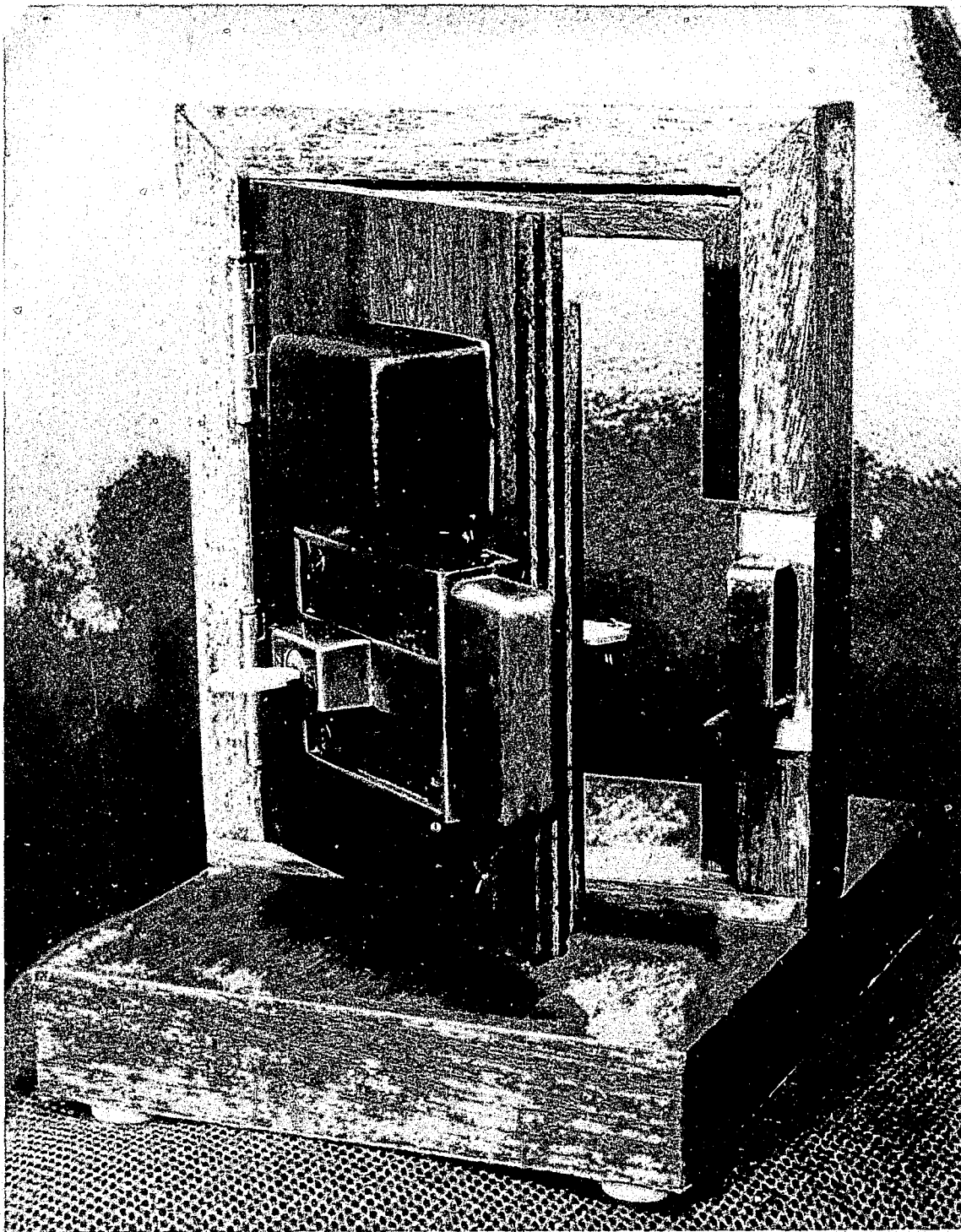


Figure 24. Deadbolt Lock, Open to Show Outside

When the system is armed, an audio alert signal is sounded if any sensor has been left open. If the situation is not corrected at the time of arming, the system will automatically ignore ("amputate") the open sensor in subsequent operation.

Outside arming activates both boundary and internal sensors; inside arming activates only the boundary sensors. Fire/smoke, emergency, and panic features are always armed. The status of the door lock (inside or outside arming) is communicated to the central controller by a miniature radio sender connected to the door switches. The occupant sets the door switches by a simple locking device with "Yes" and "No" indicators to show the condition set (Fig. 25).

Internal functioning of the deadbolt lock design is shown in Figure 26.

D. The SYNCTRAN (Synchronous Transmission) System

The SYNCTRAN system was developed specifically to meet the needs of a reliable, low-cost means of radio communication from a low-cost, adaptive system to a central response station. The SYNCTRAN concept (Fig. 27) employs a novel technique. A nearby AM broadcast station is used as a frequency reference for both the alarm transmitter and the receiver at a central location. To accomplish this, field measurements were made to establish the feasibility of the basic approach: to determine whether the propagating path between the alarm transmitter and the receiver would perturb the radio wave to such an extent that it could not be held within the narrow bandwidth desired. Such perturbations may come from automobile traffic, aircraft, moving trees, or other unknown factors. The results of the experiments showed that these perturbations were not disabling and that the basic concept was feasible.

The very narrow band radio alarm subchannels of the resulting SYNCTRAN system have a powerful concentration of radio frequency energy



Figure 25. Deadbolt Lock, Inside

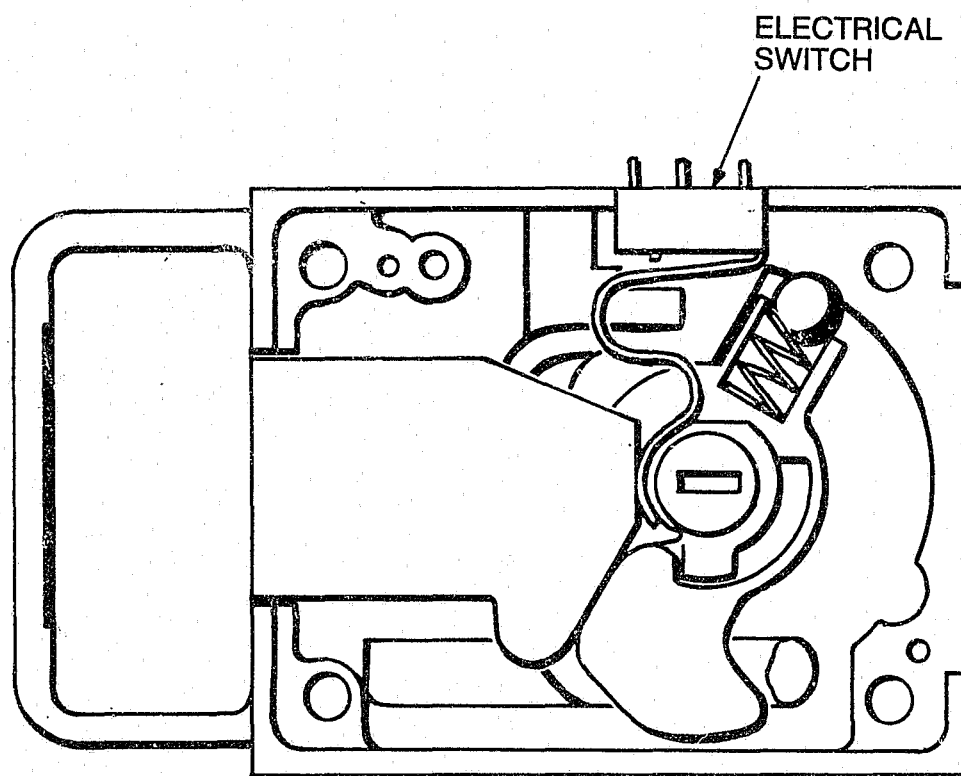
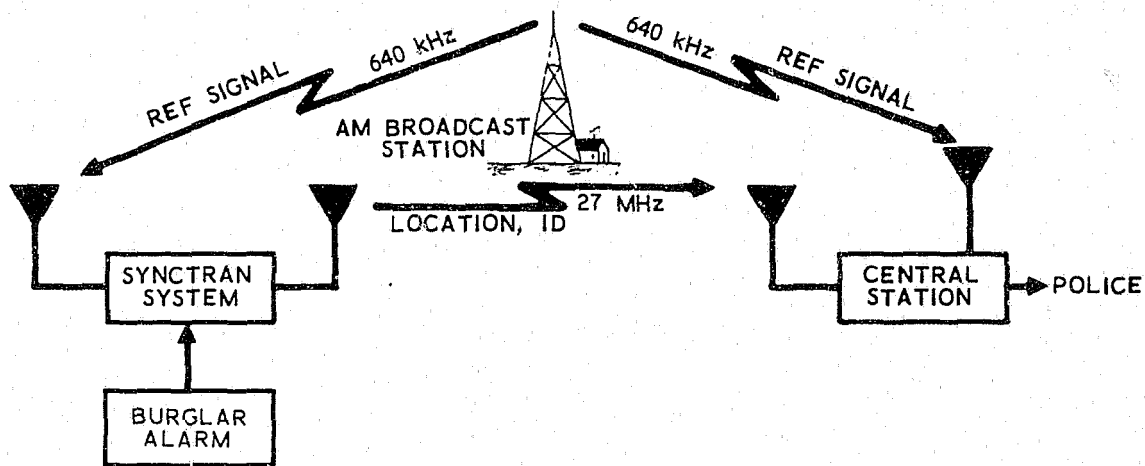


Figure 26. Internal Functioning of the Deadbolt Lock



ADVANTAGES:

- TRANSMISSION RELIABILITY
- EFFICIENT SPECTRUM UTILIZATION
- LOW COST (initial, recurring)
- NON LICENSED OPERATION

GROWTH:

- DIRECT ALARM TRANSMISSION TO PATROL CAR OR AIRCRAFT
- POLLING & PRIORITY INTERRUPT
- MOBILE TRANSMITTER (cargo security, bus)
- RADIO ALARM TRANSPONDER

Figure 27. SYNCTRAN (Synchronous Transmission) Concept

within a very small portion of the radio spectrum, minimizing the effect of both natural and manmade frequency interference. A very high signal-to-noise ratio message is obtained from a modest amount of transmitted power. The SYNCTRAN method permits a large number of alarm users to use the same radio channel, even simultaneously, without significant interference between alarm users or between alarms and voice transmissions on the same channel.

The economic and technological breakthrough that allowed development of a low-cost SYNCTRAN system was the result of successful application of large scale integration (LSI) circuitry in the SYNCTRAN frequency synthesizer, which translates the reference radio broadcast frequency into the alarm transmitter frequency. The same LSI frequency synthesizer modules would be applicable in a central receiver station (see Chapter V).

With further development, a SYNCTRAN alarm transmitter would take the form of a battery-operated package of about 3 by 6 by 1 inches in dimension. Its battery life would be about 10 years. In full production, its price would be less than \$100. It could be installed in an upper floor or attic, suspended from a 5-foot wire antenna, or an existing television antenna could be used. A detailed description of the SYNCTRAN effort is provided in Note 4.

E. Conclusion

The final products of Aerospace efforts are applicable to any system requiring the design approach established during the initial studies. The specific contributions — reliable intrusion devices, miniature wireless communication, microcomputer controller, and single point user control — all represent low-cost items compatible with operational requirements. They employ advanced technology, but are producible in quantities that use existing production capabilities. They do not represent any single system, but rather are components for a variety of systems which will increase reliability and decrease costs.

CHAPTER IV. SPECIAL REPORTS

A. Investigation of Burglar Alarm Sensors

In 1975, The Aerospace Corporation conducted a 3-month experimental investigation of selected types of sensors that could be used in burglar alarm systems for residences and small businesses. This effort was made as part of Contract No. J-LEAA-025-73 with the Law Enforcement Assistance Administration. Its purpose was to obtain data that would increase the understanding of the capabilities and limitations of various types of sensors and lead to a selection of those sensors showing the most promise of meeting the following principal program goals:

- Low false alarm rate
- Acceptable probability of detection
- Potential low cost

The following description is a summary of the Aerospace report² prepared for the Law Enforcement Assistance Administration.

1. Methodology. The following four sensor types were investigated:

- Ultrasonic
- Passive E-field
- Passive infrared
- Active infrared

The following investigative method was used for each type of sensor.

- Develop analytical models of the key performance factors
- Use modified commercial or laboratory breadboard sensors to measure human, animal, and background signatures under various conditions
- Modify the sensors to improve performance
- Measure the performance of improved sensors with a variety of targets and backgrounds

The main goal of reducing false alarms to near zero was given special consideration during the investigation. It was recognized that the operating environment of the end products would be small businesses and residences, with rooms of about 20 feet in length and as few restrictions as possible. In addition, pets running free on the premises were a consideration, and considerable effort was devoted to the measurement of signatures of moving animals and humans and the capability of the equipment to differentiate between them.

2. Ultrasonic sensors. This type of sensor is the most widely used volumetric sensor.¹ Although it has high general public acceptance, the simpler and lower cost models suffer from a high false alarm rate. The more sophisticated models have a reduced vulnerability to false alarm sources, but no commercial models are capable of discerning the difference between a small animal and a human in the target range. Present commercial designs do not avoid alarms caused by mechanical noises occurring at discrete frequencies readable by the sensor as a target.

a. Method of detection. The technique of using ultrasonic energy to detect an intruder is based on a principle similar to sonar used for underwater detection of reflecting bodies. The method exploits the fact that any object greater in size than a few wavelengths of the impinging acoustic energy will reflect that energy with relatively low loss. At the ultrasonic frequencies of 20,000 Hz or more, the critical dimensions are in the order of inches or fractions of inches. In addition, if the reflecting surface is moving with a radial component with respect to the source or receiver, it will modify the frequency of the energy seen at the receiver. This effect, called the Doppler effect, provides a convenient mechanism to separate energy reflected from stationary surfaces from energy reflected from surfaces in motion. It is the energy received with a modified, or Doppler, frequency that is used in nearly all ultrasonic alarms. If the receiver merely used the increase, or decrease,

of a reflected energy level caused by a change in reflector configuration, it would be more suitable to be used in a volume where there is very little reflection from the enclosing walls. However, if the room is about the dimension of the desired detection distance, the level of undisturbed reflected energy is high, and any disturbing reflection represents only a small change in received energy. Use of the Doppler effect permits the receiver to ignore the normal stationary reflections and to detect with high sensitivity any received energy at a modified frequency caused by a moving reflector. Most commercial units operate on the detection of the Doppler modified reflections and are able to detect humans moving at ranges of 25 feet or more. The analyses that follow provide quantitative values for reflection coefficients, various losses that occur between the transmitter and receiver, and the Doppler frequency magnitudes.

The Doppler frequency generated due to radial components of velocity of a reflector are shown in Figure 28. It should be pointed out that the radial velocity component is with respect to the energy source and receiver and not necessarily via the direct path. Energy reflected from walls, floors, etc. also acts as sources. The total Doppler signal received is a composite of the direct rays and any energy transmitted and received in a multipath manner. The multipath-received energy is lower in intensity than the direct signal since it suffers a greater range loss. But, in general, when a body moves in a closed volume illuminated by acoustic energy, the Doppler responses are not entirely due to the direct path rays. Doppler frequencies both above and below the carrier frequency can be expected. This fact makes it almost impossible to a priori establish a frequency spectrum signature for a human body. Considering the range of velocities, the directions of motion, and the multipath scenario, only rough filter limits can be applied to the Doppler frequencies generated by a human intruder. However, several conclusions can

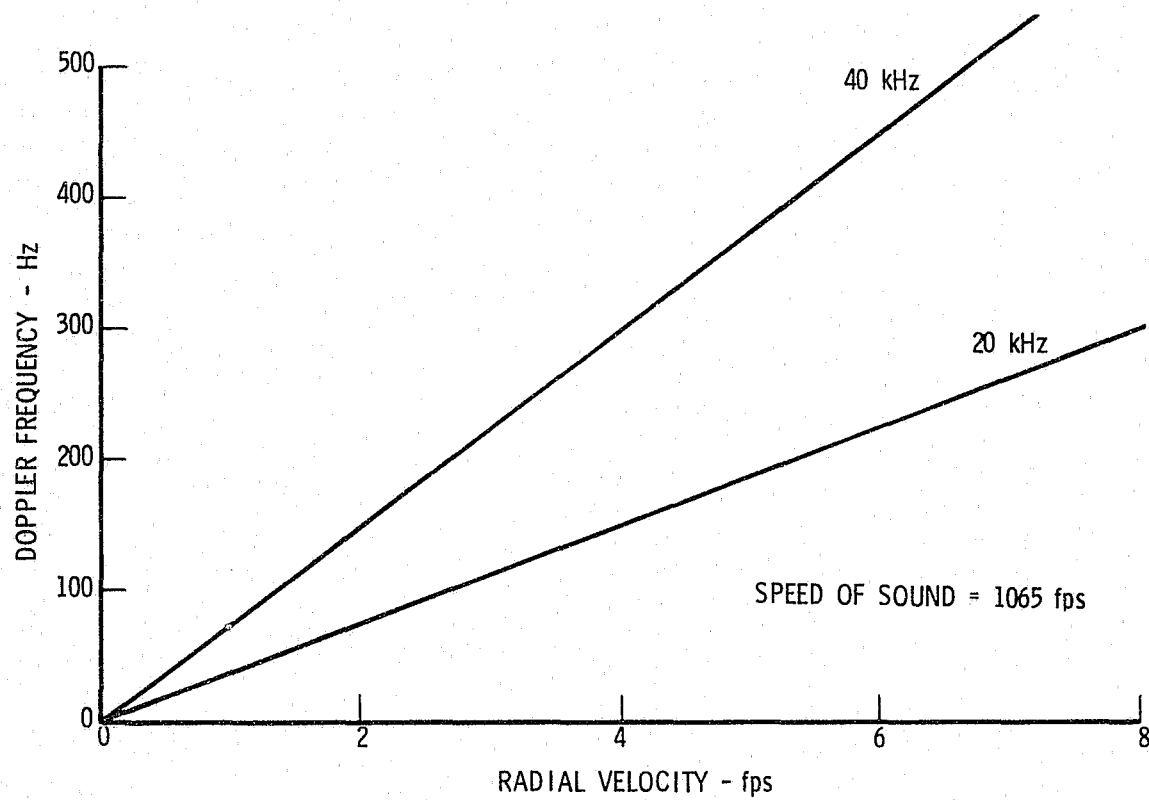


Figure 28. Doppler Frequency

be made: (1) the direct-ray-path Doppler frequency will be the greatest intensity; (2) a single human will generate Doppler frequencies that are not of equal intensity on each side of the carrier frequency; and (3) the Doppler returns from a human will be similar over the ultrasonic band of 20 to 40 kHz in percent of the carrier frequency.

b. False alarms. Several causes of false alarms were considered and delineated by their Doppler and spectral characteristics.

Oscillating reflectors, such as lamps that are wind blown or windows that rattle, are expected to generate Doppler signals that vary in polarity with time. An integral of their Doppler frequencies, with polarity maintenance, should provide a mean value near the carrier frequency.

Reflections from hot-air turbulence should be relatively uniformly distributed across the band of both positive and negative Doppler signals. A simple subtraction of the two polarities of Doppler signals should eliminate such returns. Thus, for the two cases above, an integration of each Doppler sideband, followed by a simple differencing of the positive and negative outputs, should eliminate signals from those sources. However, that technique would not eliminate any noises that occur in only one Doppler sideband. Since these noises are naturally narrowband in character and since they are not the result of a Doppler effect, they would not be expected to appear in the same polarity sidebands of two carrier frequencies. Thus, the use of two carriers spaced by about 10 kHz can be used to establish the existence of a true Doppler signal.

The overall rationale to eliminate false alarms is as follows:

- Process, integrate, and evaluate the Doppler frequency returns both above and below two carrier frequencies.
- Compare the intensities of the positive and negative Doppler signals for each carrier. A human intruder alarm will be established

when above-threshold differences between the sidebands are noted for both frequencies for the same polarity. Sources that generate sidebands at about the same magnitude would be considered false alarms.

- The integration period of the process is to be established experimentally, although the choice of from 5 and 10 seconds should not be too critical

In the case of very small animals, it is possible that the return signal strengths will differ enough at the two carrier frequencies to permit recognition of the animal. This will not work for animals that reflect equally well in both carrier frequencies. That case can only be avoided by not illuminating the volume occupied by the animals.

c. Testing. There were four testing objectives:

- To evaluate the false alarm sensitivity of one of the better commercial units
- To establish that a heterodyne and filter technique could be used to separate the positive and negative Doppler signals
- To evaluate some typical spectral densities of human motion
- To appraise the breadboard model designed to separate the Doppler signals

The results of false alarm tests are presented as Table 2. The tests were run with maximum range sensitivity settings and with a wide-beam diffruser. The commercial unit was also under observation during periods when valid alarms were either purposefully or inadvertently generated. There were no known cases when the unit failed to alarm at ranges to 25 feet, even in cases where it was not in the direct line-of-sight. All attempts to "inch by"

Table 2. False Alarm Test Summary, Conventional Unit (26.5 kHz)

Scenario	Height (feet)	Range (feet)	False Alarm (%)
Home - 25-lb dog	4	3-15	100
Home - 35-lb dog	4	3-15	100
Home - 25-lb dog	7	3-15	50
Home - 35-lb dog	7	3-15	75
Office - key jangle	3	3-10	75
Office - telephone	3	4-30	None
Office - moving drapes	3	4-10	None
- moving plastic material	3	10	100
Home - hair dryer			
- tangential	4	3-6	50
- radial	4	3-6	100
- tangential	4	10	0
- radial	4	10	25
A-1 basement - motor noises	3	2-12	0

the unit failed. However, as Table 2 indicates, the unit also responded to the dogs used as test specimens. The failure to alarm in some cases was due to the movements of the dogs behind or under furniture. The hair dryer that was used to generate false alarms contained a 750-watt heater and only caused alarms when the heater was activated.

d. Breadboard model. A transceiver was designed and constructed to receive and separate the Doppler signal returns (see Fig. 29). This transceiver separated the positive and negative Doppler signals as opposite polarity outputs; it is described in an Aerospace Corporation internal report (ATM-76(7904)-1) written by W.D. Harmon and published in July 1975. An estimate of the parts required for an ultrasonic burglar alarm system sensor using the separated Doppler channels and two carrier frequencies is shown in Table 3.

e. Conclusions. Results of the investigation indicate that the ultrasonic sensor, though a sensitive and high-confidence device to detect human motion, is also vulnerable to several forms of false alarms. Some of the causes of false alarms can be minimized by careful installation, but it does not appear feasible to avoid alarms caused by the illumination of medium to large pet animals. The use of a dual frequency system with separate Doppler channels appears to be feasible, and the exploitation of the available data permits additional processing to reduce vulnerability due to some other causes of false alarms. The cost of a dual-carrier frequency system is estimated to be at a level that does not permit it to be retailed at "under \$50."

3. Passive E-field sensors. E-field intrusion sensors operate on the following two physical principles:

- Sensing of the static charge accumulation on a nonmetallic body
- Change in capacitive coupling of an antenna to the earth.

During low-humidity conditions, any animal will generate upon its body a large static charge from its movements. The static charge becomes especially large if a person or pet moves on a typical carpet or if a person is

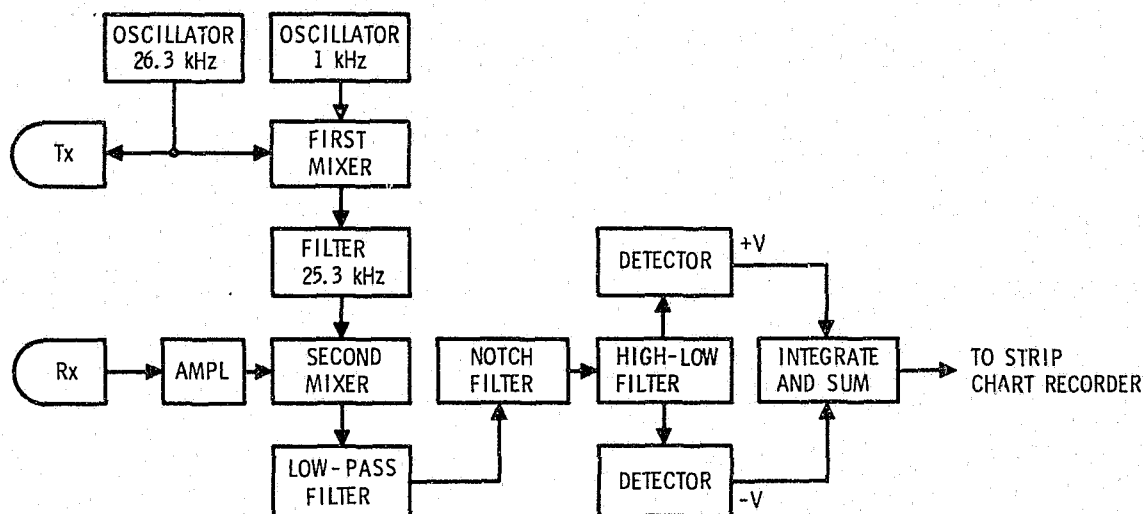


Figure 29. Block Diagram of Breadboard Ultrasonic Alarm Sensor

Table 3. Advanced Ultrasonic Burglar Alarm Sensor Parts Count and Costs

Item	Number Required	Approximate Cost (\$)
Transducers	4	16
Active microcircuits	20	12
Passive components: resistors, capacitors, diodes	100	5
Power supply components: transformer/battery	-	3
Hardware: printed circuit board, case, switches	-	2
Total		38

wearing certain types of clothing. It is possible (by using a very sensitive low frequency receiver) to sense the electric field produced by a body's static charge (by means of additional electronic sophistication) to detect a fluctuation in the body charge that accompanies animal movements.

In addition to accumulating a static charge, all animals cause a distortion in the Earth's electric field. The generated field distortion arises because living creatures do not have electrical properties identical to the surrounding atmosphere; primarily with respect to electrical conductivity and dielectric constant.

The distance, the area, or the volume within which these E-field signals may be sensed can be controlled by selecting the length of wire attached to the input of the special high-impedance receiver. Small antennas usually produce a confined zone of detection for an E-field sensor.

By taking advantage of the differences in body movement rates between humans and pets (primarily the number of foot-to-floor contacts per unit distance), added discrimination is designed into the more sophisticated types of E-field sensors.

a. Experimental and theoretical efforts. The supporting experimental program consisted of measuring the moving, passive E-field signatures of humans and animals in residential and business indoor environments. Two specialized, high impedance, low frequency linear amplifiers — a Keithly electrometer and a modified Stellar intrusion detector — were used to obtain and magnetically record several hundred moving signatures of 17 people and eight small pets in four private residences and one office building. The signatures were recorded for targets walking at known distances and speeds from both sensor types. Auxiliary measurements of both the Earth's ambient electric field and the electrostatic potential on the subject were made. Target speeds varied from a fraction of a meter/second to about 1.5 meters/

second. Substantial variations in subject footwear, clothing, floor surfacing, furnishings, and building construction are reflected in the data.

The magnetic recordings were automatically digitized, amplified, and plotted for high-resolution inspection and power spectral density computations. Samples of these signatures and the associated power spectral densities are shown in Figures 30 and 31. Finally, manual analyses were performed on the digitized signatures and associated power spectral density presentations to extract the statistics of false alarm and false dismissal rates. False alarm and false dismissal rates were established for several configurations of possible discriminators and detectors to obtain the best functional combination, i. e., the lowest false alarm rate combined with a low false dismissal rate.

The associated theoretical effort consisted of the computation of the ambient electric field perturbation caused by the presence of a symmetrical, charged dielectric body, representation of either a human or animal as a function of the electrical and geometrical parameters of the body, the distance from the body and the ambient electric field intensity. An example of this computation is the curve marked Theoretical Predictions in Figure 32.

The experimental points showed agreement with the predicted trend, although the absolute amplitude was normalized to the calculated value. This was necessary because the gain, or scale factor, of some of the test equipment (for example, the antennas) was not calibrated. Notice that the falloff of signal with range is much faster than $1/R^{-2}$.

The results of these computations guided portions of the experimental program and, in addition, were employed to establish functional parameters of the discrimination and detection circuitry, where experimental corroboration permitted extrapolation.

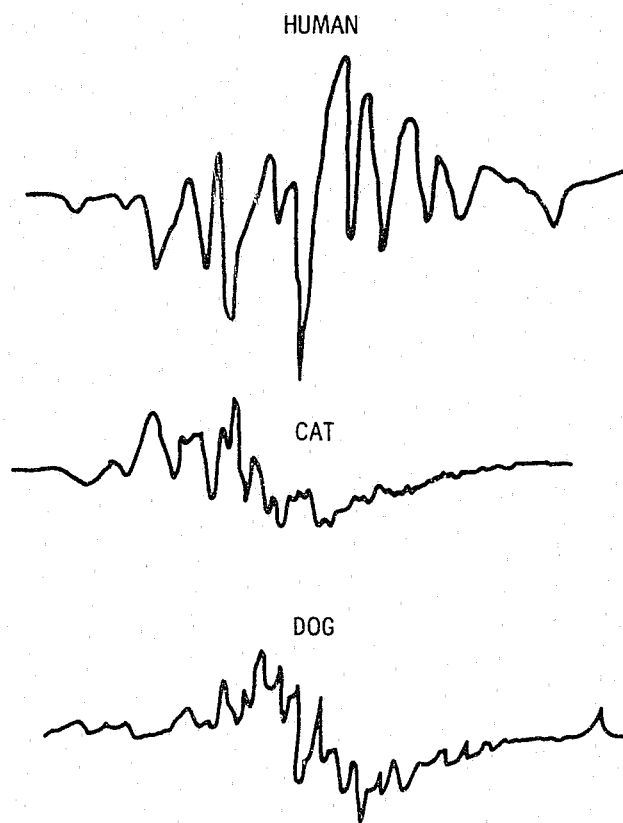


Figure 30. Time History of Outputs

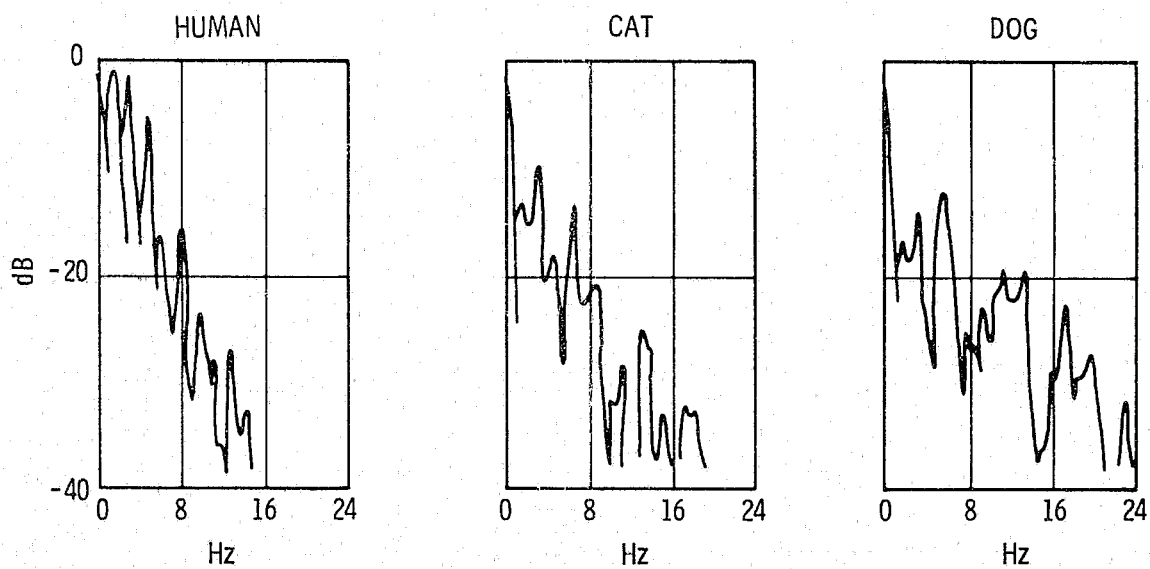


Figure 31. Power Spectral Densities

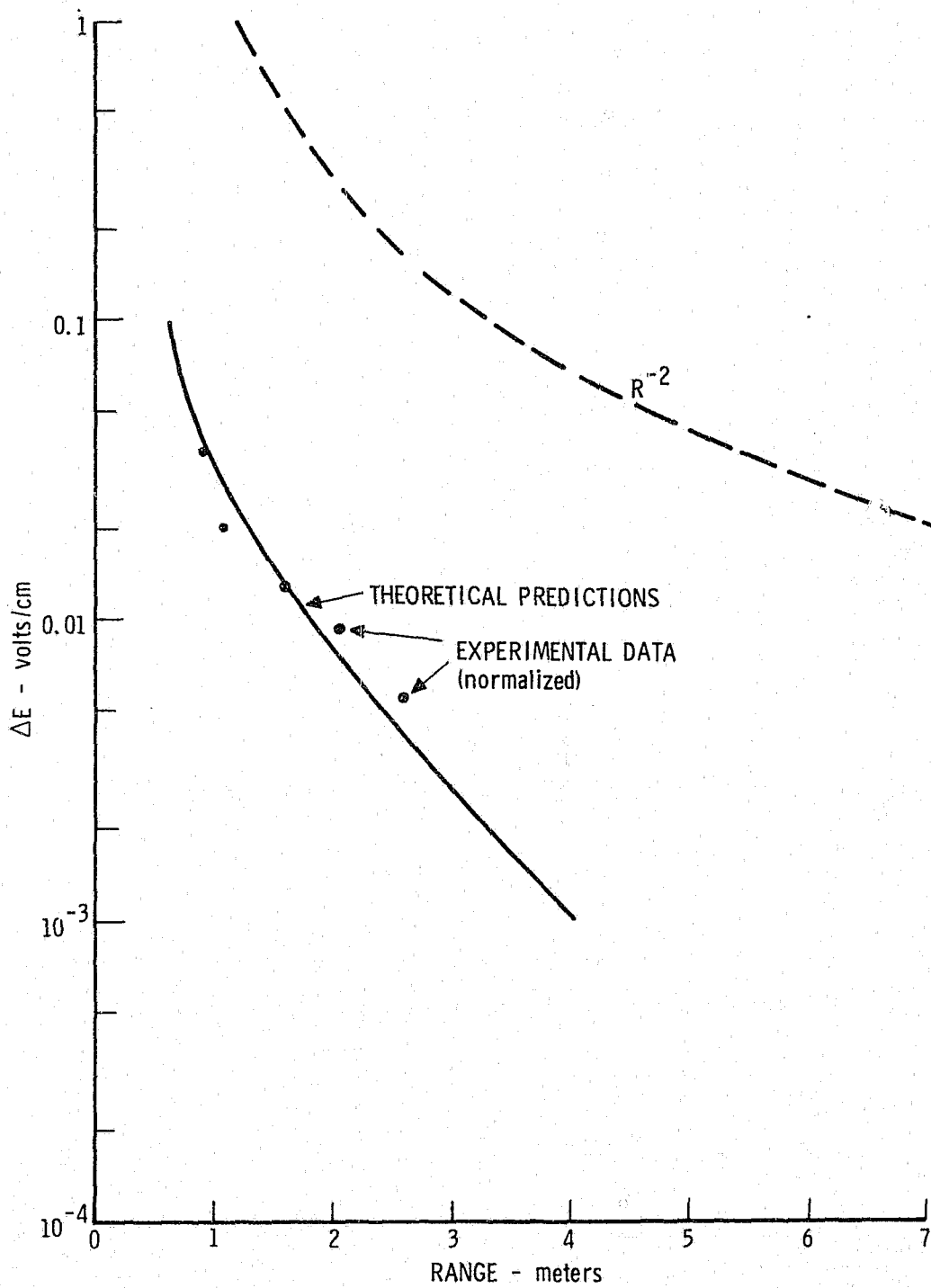


Figure 32. Comparisons of Measured and Computed Mean E-Field Signature Variation with Subject Range from the Detector

b. Performance analyses of discriminator and detector options.

The following three discrimination concepts were initially considered:

- Correlation
- Zero crossing rate
- Band filtering and threshold detection

The correlation discriminator option was abandoned after examination of human signatures revealed that great pattern variability exists even between the signatures of one person or one animal moving in the same local area. The possibility of establishing a reference pattern for humans or animals is remote.

A zero-level-crossing-rate detector, providing an event count in a precisely establishable interval during the passage of the target near the sensor, was found, by analytical test against the signature data base, to be capable of yielding a low false dismissal rate. The majority of animals tested yielded a zero event count during a 1-second postmaximum interval.

Because some pets were observed to yield a nonzero critical count during the 1-second postmaximum interval, the zero level crossing rate was functionally combined with the third listed discriminator type. The functional form of the ratio detector is representable by a pair of filters, each of which feeds a peak power detector. The peak power detectors, in turn, feed a ratio detector biased with respect to the internal noise level. The ratio \mathcal{R} of the low-band to high-band filter output is developed, and an event defined when \mathcal{R} exceeds a preset threshold L_B .

Finally, the event count of the zero level crossing rate and ratio discriminators are combined in an "AND" gate logic circuit to provide a "1" output when a human intruder approaches the sensor.

Values of the operating parameters of the zero-level-crossing-rate and ratio detectors were selected for computing false alarm and false dismissal using the signature data base. The most significant results are summarized in Table 4.

Examination of Table 4 reveals the following key points:

- Both zero-level-crossing-rate and ratio detectors are required to achieve a minimum false alarm.
- The value of L_B should be less than 10 decibels to minimize false dismissal. (Further, it should not be less than 8 decibels to avoid thermal-noise-triggered false events exceeding 1 percent).
- Ratio (or amplitude) discrimination only is the least effective, yielding very high false alarm and false dismissal rates.

c. Function features of the recommended E-field receiver design.

From the statistical analysis summarized in Table 4, a set of functional characteristics of the best discriminator/detector circuit was derived and is as follows:

- Input Section*
 - $R = 10^9$ ohms
 - Minimum cable length, 3 feet
 - Circuit time constant less than 10^{-2} second
 - 60-Hz reject filter, notch loss exceeding 60 decibels
- Discrimination and Detection Circuit
 - Two-mode discrimination: (1) positive crossing rate, and (2) tuned ratio detector
 - Crossing rate detector: envelope detector, limiting circuit, zero-time reference circuit, and zero crossing counter

*The input characteristics are necessary to achieve the needed bandwidth and an adequate pickup probe length.

Table 4. Statistics Summary

Target	Discrimination with Zero Level Crossing Rate Count Only				Discrimination with Ratio Only					Discrimination with Zero Level Crossing Rate and Ratio			
	Count $> \frac{C}{C}$	No. of Cases	0's	PD	LB	Low-Band Filter Type	No. of Cases	0's	PD	Count $> \frac{C}{C}$	No. of Cases	0's	PD
Men	0	80	3	0.96	7	BP	144	28	0.81	1	80	25	0.69
					7	LP	144	19	0.87	1	80	24	0.70
										0	80	10	0.88
					8	LP	144	20	0.86	0	80	11	0.86
					10	LP	144	42	0.71	1	80	30	0.63
										0	80	17	0.79
Women	0	26	0	1.0	7	BP	49	10	0.80	1	26	8	0.61
					7	LP	49	8	0.84	1	26	7	0.73
										0	26	2	0.92
					8	LP	49	8	0.83	0	26	2	0.92
					10	LP	49	14	0.71	1	26	8	0.69
										0	26	5	0.81
Animals	0	13	11	0.15	7	BP	30	10	0.67	1	13	11	0.15
					7	LP	30	10	0.67	1	13	11	0.15
										0	13	11	0.15
					8	LP	30	13	0.57	0	13	12	0.08
					10	BP	30	17	0.43	1	13	12	0.08
										0	12	12	0.08

- Tuned ratio detector assembly: low-pass filter and peak power detector plus bandpass high frequency filter and peak power detector, ratio detector
- Logic circuitry: "AND" circuit with crossing rate (CR) and (R) inputs. Decision intruder if CR and R both exceed set limits, \underline{C} and L_B

• Parameters

- $\underline{C} > 0$
- $L_B = 8 \text{ decibels} \pm 1 \text{ decibel}$
- CR greater than zero during 1-second postmaximum of of signal envelope
- Zero time reference - signature absolute maximum
- Filter roll-off
- Peak power detectors set for 3 decibels above noise threshold
- Minimum dynamic range (linear $\pm 0.5 \text{ decibel}$) peak power detectors = 45 decibels
- Minimum dynamic range (linear $\pm 0.5 \text{ decibel}$) ratio detector = 10 decibels

4. Passive infrared systems. All objects not at a temperature of absolute zero emit infrared radiation, but the wavelength and intensity of the radiation depend on the nature of the object. Most objects related to human habitation are generally at an ambient temperature of approximately 23°C (73°F), while the human intruder is generally at a temperature of approximately 37°C (98.6°F). The peak of the radiant emittance from the objects within these temperature ranges varies from approximately 9 through 11 micrometers.

There are certain basic components generally common to all infrared systems regardless of the area of application for which they are designed. These systems have an optical system for collecting radiant energy from the target of interest and for focusing this energy upon a detector that converts the energy into an electrical signal. An electronic system amplifies the detector output signal and processes it to a form that can be used as an intruder alarm.

Infrared radiation provides a means of measuring temperature at a distance from the object since the radiation is dependent upon the object's temperature. Objects so hot as to be incandescent can be thermally measured by very simple infrared radiometers, or they can be photographed by so-called infrared film, which operates in the very-near infrared spectral region. Objects only moderately warmer than the normal indoor environmental temperature present the most difficult measuring problems. The radiation has insufficient energy to produce the necessary chemical change in photographic film — even the so-called infrared type.

The warming effect is one of the two* principal mechanisms for the detection of infrared radiation. An extremely small flake of absorptive material in a carefully designed thermal structure is able to rapidly attain an equilibrium temperature dependent upon the incoming radiation. If the flake

*Another widely employed type of infrared detector is the photon detector. In this device, an electrical carrier is produced in a semiconductor by the direct action of a single photon of incoming radiation. Such devices are characterized by high spectral sensitivities and by abrupt long-wavelength cutoffs of sensitivity. This detector requires cryogenic cooling to perform satisfactorily and is not used in commercial burglar alarm units.

material has a usefully large temperature coefficient of resistance, the infrared-induced thermal change will cause an electrical signal in an associated circuit. An infrared detector of this type is called a thermistor bolometer.

All radiation measurements involve comparison with a reference standard. The detector measures the radiation difference between the source radiation (human) energy focused upon the detector and the radiant energy reference (room and surrounding objects) level in the infrared device. This is accomplished by using two detectors viewing the same field of view.

a. Tests and evaluations. Of the several systems available, two were tested and evaluated.

The Barnes Engineering Company Infraguard passive infrared sensor detects infrared radiation of a moving intruder using a logic system that differentiates this signal from other thermal sources in the protected area and produces an alarm signal.

A total coverage of 70 degrees horizontally and vertically is provided. The detector divides this protected area into 10 guarded zones. As an intruder moves through the protected zones, his radiant energy produces positive and negative signals alternately. The logic circuitry determines that these signals are from an intruder instead of from spurious thermal sources. The combination of the lens and its optical coating helps to eliminate solar radiation and energy coming through glass windows.

Three target velocities at three ranges were used in the evaluation. The human target moved across the zones of protection at distances from the sensor of 3.8, 9.8, and 19.7 feet. These distances corresponded to object space dimensions of 0.5 by 1.6, 1.4 by 4.7, and 2.8 by 9.5 feet, respectively. Intruder velocity was estimated by the length of time it took the target to travel between two prescribed marks. These velocities were approximately

1.3, 2.5, and 6.2 feet per second. The autocorrelation function obtained from the data taken at the range of 20 feet were 1.4, 2.5, and 11.6 feet per second, respectively.

The power spectral density plots show that, for a velocity of 1.3 feet, the major peak of the received energy occurred at approximately 0.2 Hz, with a secondary peak located at approximately 0.75 Hz (Fig. 33). When the velocity was increased to 2.5 feet per second, the major peak shifted to approximately 0.5 Hz, with the secondary peak showing up at approximately 1.4 Hz (Fig. 34). At the velocity of 6.2 feet per second, the major peak shifts to approximately 2.2 Hz (Fig. 35). The velocity calculated by using the autocorrelation function for the high velocity is probably in error because of the time constant of the detector and the probability of error in determining the exact location of peaks.

Additional tests were performed on a qualitative basis to evaluate the system's susceptibility to nuisance alarms such as light bulbs, solar energy, electric heaters, electrical disturbances, noise, and vibration. It was found that the system was not susceptible to noise vibration, electrical disturbances, flashlights, and light bulbs; however, it responded intermittently to the cycling of an electric heater and movement of objects illuminated by solar energy. The electric heater and solar energy tests were repeated after a filter having a bandpass from 8.4 to 12.4 micrometers was mounted in front of the aperture. The solar energy problem was eliminated, and the response to the electric heater was substantially reduced.

The Infraguard system detected an intruder to distances of 40 feet, even when it was operated outdoors.

The Rossin Corporation Thermal Intruder Sensor (Fig. 36) responds to thermal-radiation changes it sees when an intruder moves across the area viewed by the sensor. The intruder can be either warmer or cooler than the

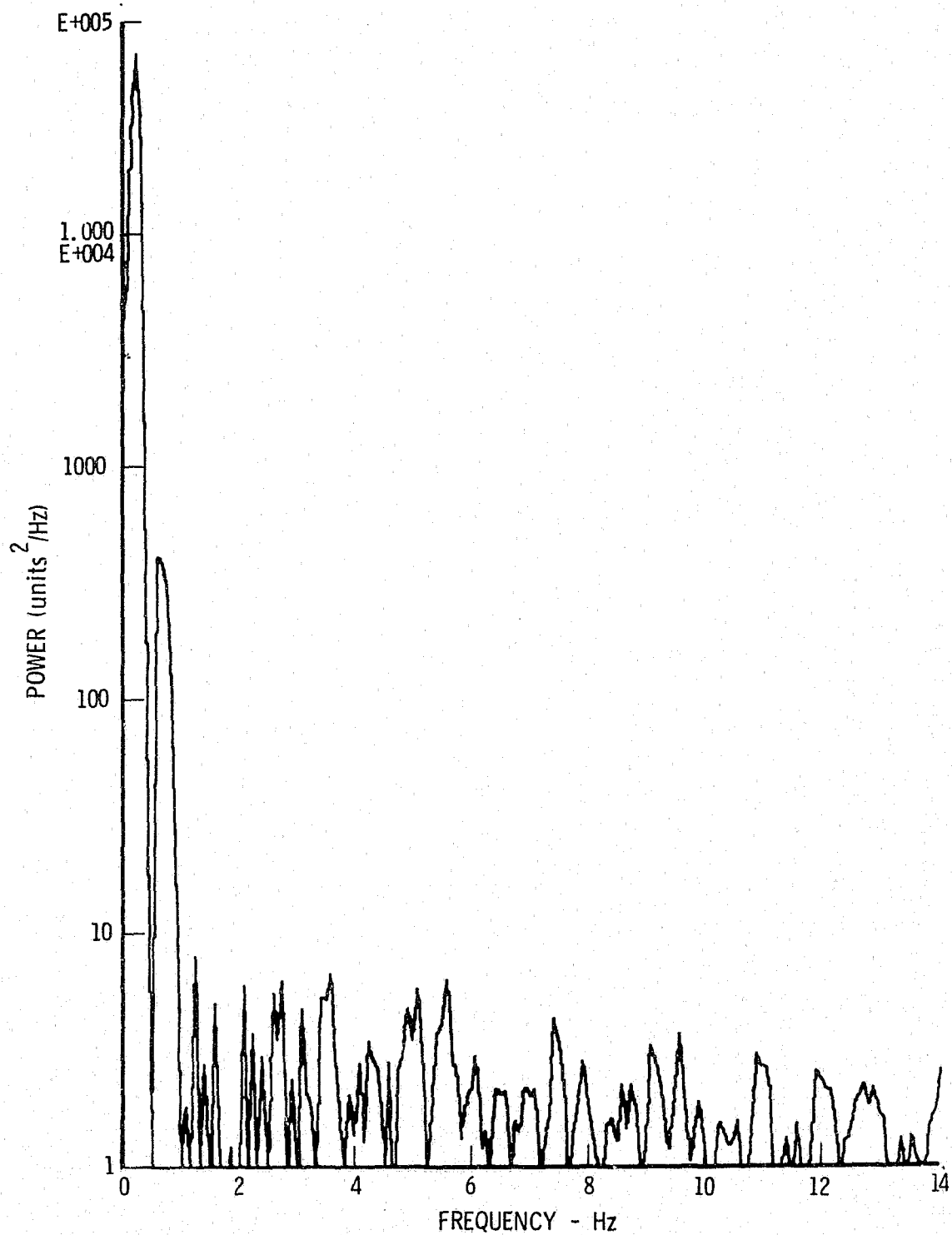


Figure 33. Power Spectral Density (Intruder Velocity
1.3 Feet Per Second)

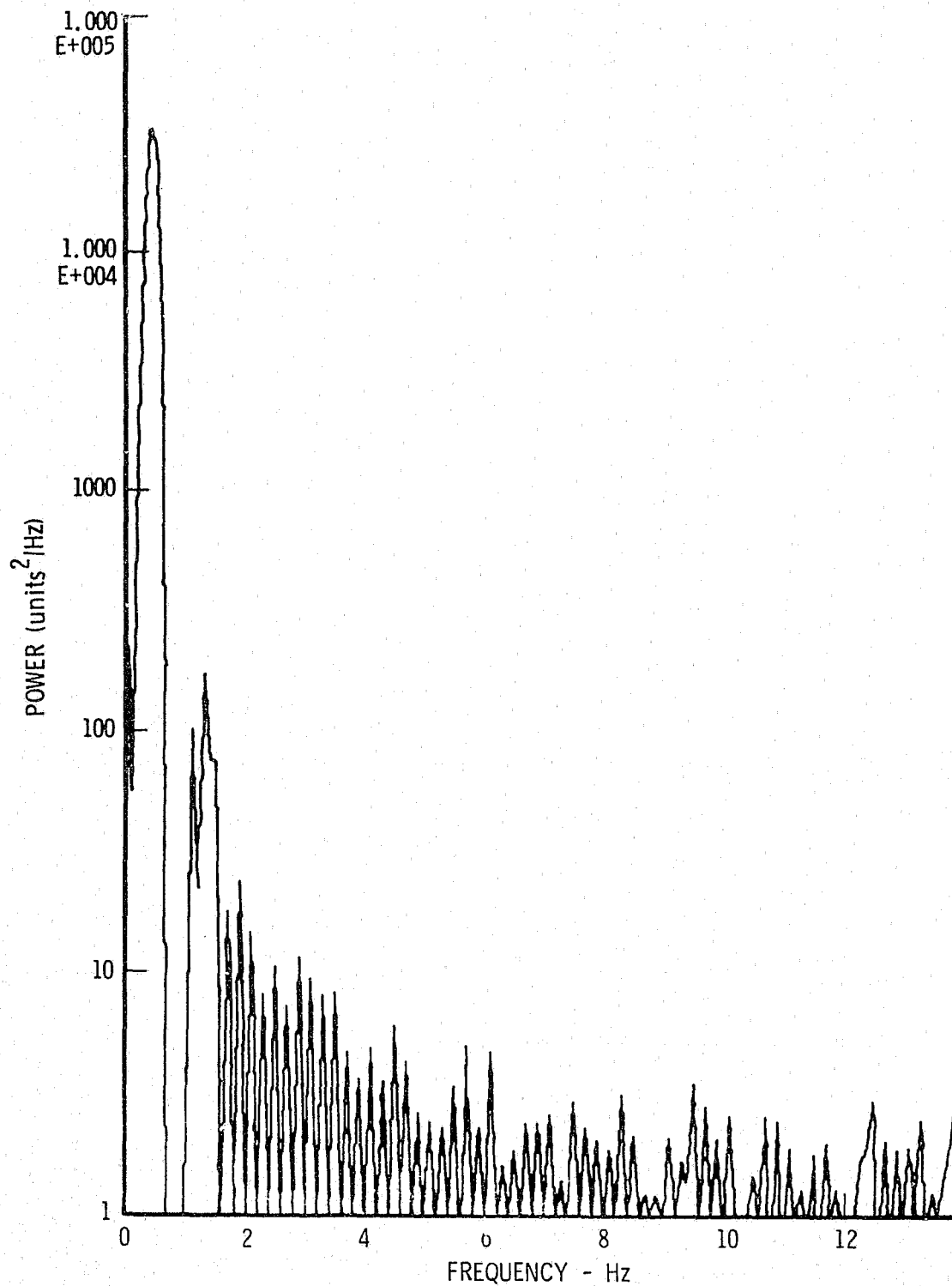


Figure 34. Power Spectral Density (Intruder Velocity
2.5 Feet Per Second)

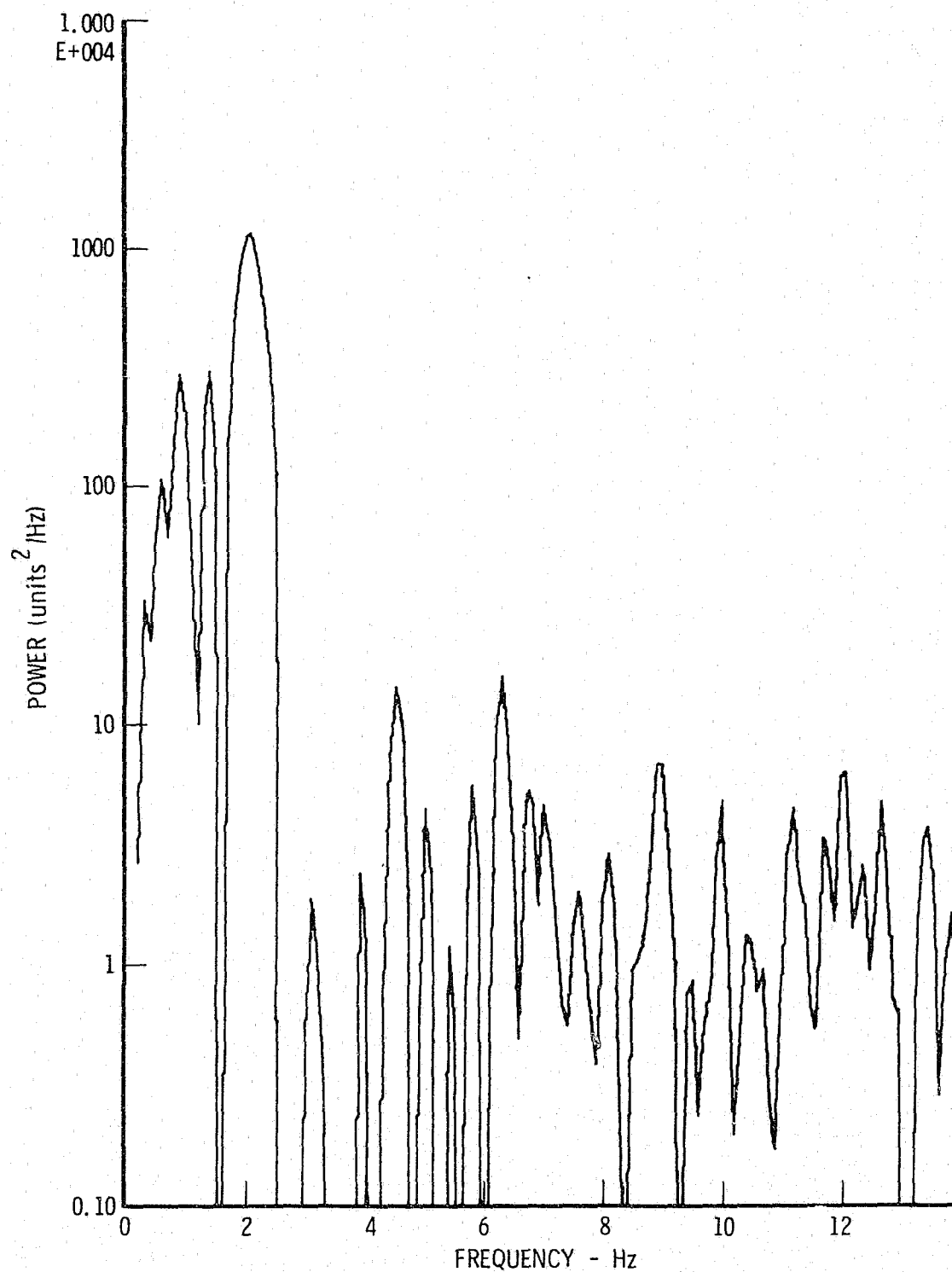


Figure 35. Power Spectral Density (Intruder Velocity
6.2 Feet Per Second)

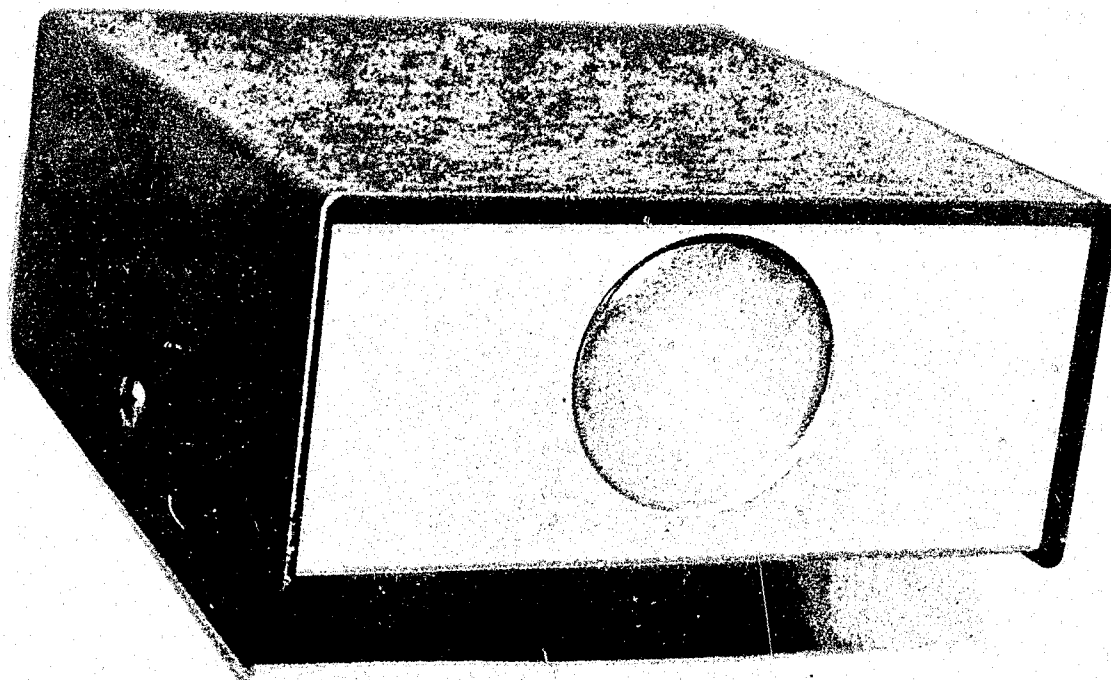


Figure 36. Rossin Corporation Thermal Intruder Sensor

ambient environment. The field of view of the sensor is approximately 2 feet in diameter at 50 feet. When an intruder moves through the field of view, the logic relay will latch on for 1 second and then will not be usable for an additional 20 seconds.

The Rossin Corporation unit readily detected an intruder at approximately 25 feet. Detection took place under high ambient light levels as well as low ambient light levels. As indicated in the literature,³ false alarms were noted when changing sunlight conditions were allowed within the limited field of view.

b. General conclusions. From the power spectral density curves, it is apparent that the upper frequency cutoff need not be higher than 3 Hz. The lower frequency cutoff should be below 0.2 Hz to detect a very slow moving intruder.

From the false alarms under sunlit conditions, it is apparent that one should either utilize the currently expensive long-wavelength infrared cut-on filters or limit the field of view to avoid this potential source of false alarms.

From the ability to induce false alarms by having an electric heater directly in the field of view, it is apparent that there is a tradeoff between extensive field-of-view coverage and false alarm rate. It is recommended that the field of view be confined to the minimum amount necessary for protection. This amount necessary for protection is a function of the anticipated sophistication of the burglar and the area being protected.

5. Active infrared systems. In the course of the investigation, active infrared technology was examined to see if it could be applied to obtain an effective burglar alarm sensor with a low false alarm rate and a potentially low cost. The approach to meeting this objective included the following:

- Soliciting and evaluating technical information from manufacturers of commercially available intrusion detectors

- Procurement and testing of two commercial units
- Study of infrared light-emitting diode (LED) and silicon detector characteristics

a. Guidelines. Several guidelines that influenced the direction of efforts (besides the required low false alarm rate) were recommended by the Aerospace Program Office. First, the sensor should be low in cost, including installation expenses. Second, the installation should have no need for items that would be objectionable from an esthetic point of view. Third, it would be desirable to obtain better coverage of room volume than that afforded by a single-beam active device. In following these guidelines, the concept evolved of utilizing a multibeam, active infrared sensor that would detect the presence of a moving intruder by measuring the average signal obtained from reflection from a wall or an object and triggering the alarm when this average was either increased or decreased as the intruder entered the beam.

The guidelines eliminated several candidate sensors. In particular, the single beam-interrupt concept, with a transmitter pointing across the room to a separate receiver, was considered unacceptable because of the lack of volume coverage and the expense of installation. Also considered unacceptable was a multibeam system, using cooperative reflectors (mirrors, retroreflectors, reflective tape) because of installation restrictions and esthetic considerations. A single beam unit, producing two or more crisscrossing beams by means of carefully adjusted mirrors, was considered unacceptable for the same reasons and because of the possibility of a high false alarm rate due to mirror movement from sonic booms, earth tremors, or vibration from other causes.

b. Summary of activities and accomplishments. Activities and accomplishments included the following:

- Technical information on commercially available intrusion sensors and components was obtained and studied.

- Infrared light-emitting-diode and silicon detector characteristics from several manufacturers, including RCA, General Electric, EG&G, Texas Instruments, Fairchild Semiconductor, Meret Inc., United Detector Technology, and Bell and Howell, were reviewed.
- Two commercial, active infrared burglar alarm sensors (the Photomation Model TR-8-01 and the Detection Systems, Inc., Model DS-300) were procured for evaluation.
- Three active infrared sensor concepts were breadboarded, and one of these was developed into a "brassboard" unit (Figs. 37 and 38).
- A means for obtaining multibeam operation with a single light-emitting-diode and a single silicon detector was invented and implemented, offering improved coverage without significantly increasing costs. (A patent disclosure is planned.)
- Tests were devised and conducted to determine capabilities and limitations of commercial and Aerospace-developed units.
- Through the cooperation of Mr. David Lederer, Vice President, Operations, Detection Systems, Inc., schematic diagrams and descriptive material were obtained to permit understanding of the operating principles of their active infrared burglar alarm.
- The relative reflectance of 14 surfaces, including wall materials, woods, and clothing, was measured using the Aerospace sensor as a test instrument.

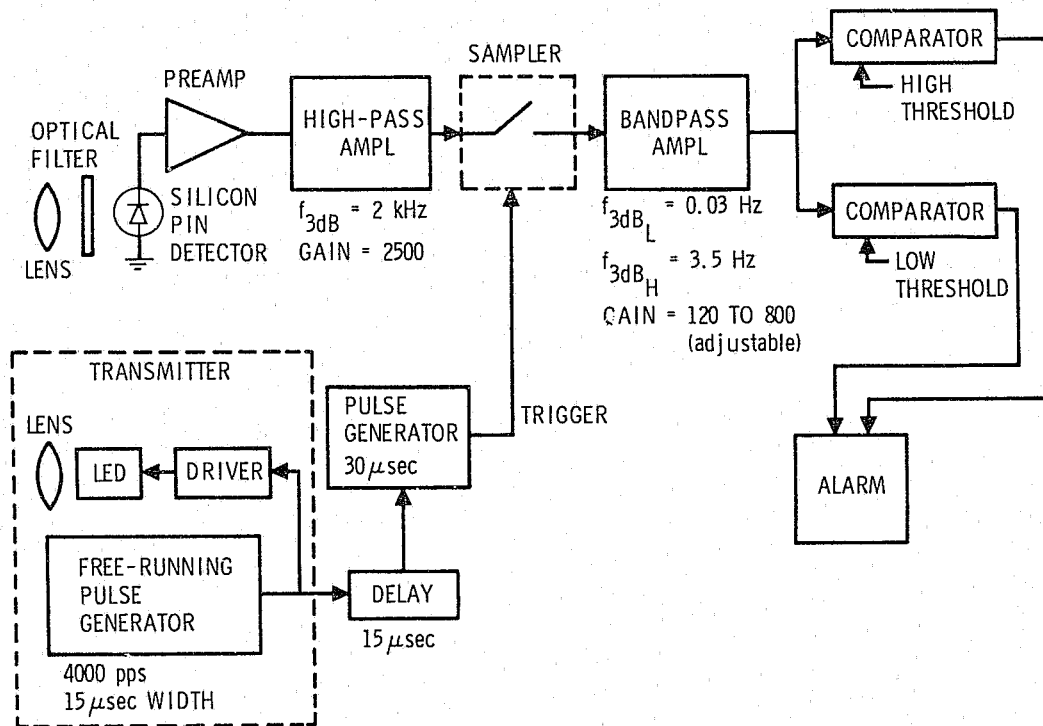


Figure 37. Block Diagram of the Aerospace Active Infrared Burglar Alarm

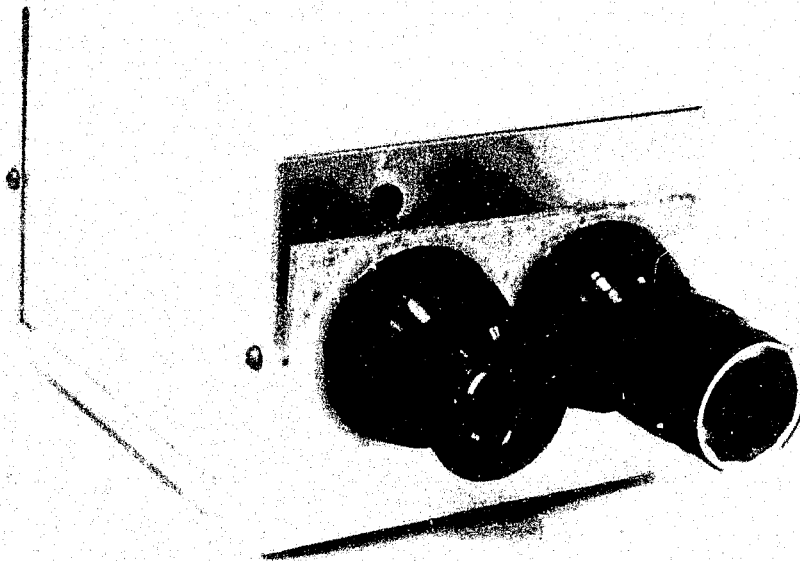


Figure 38. The Aerospace Active Infrared Burglar Alarm

c. Applicability of active infrared systems. After study, analysis, development, test, and evaluation, it was concluded that an active infrared burglar alarm sensor can be effective and reliable, can have an acceptably low false alarm rate if properly designed and installed, can be relatively immune to countermeasures, and is potentially low in cost, based on continuing developments in gallium arsenide and silicon technology and use of simple glass or plastic optics.

The active infrared unit developed by The Aerospace Corporation operates satisfactorily and can be substantially improved in performance and reduced in cost by relatively minor changes in the optics and electronics. In particular, the multibeam configuration is considered promising.

One commercial unit (Detection Systems, Inc., Model DS-300) provided good single-beam performance and could be used (as manufactured, or with minor modifications) as one sensor of a complete burglar alarm and communications system to expedite system testing.

6. Conclusions. All four types of sensors were capable of adequate detection performance against human targets. The passive E-field sensor has limited range and appears reliable only up to about 12 feet. Also, variability in target signatures resulted in a measured probability of detection of about 0.9. All other sensors tested exhibited essentially 1.0 probability of detection at distances of up to about 25 feet.

A major finding of the experimental program is that sensors having a wide field of view, i.e., those that "see" a large part of the room volume, will be susceptible to false alarms in an unrestricted home environment. Discriminants determined from measured signatures appear inadequate to reduce these to an acceptable level. Specifically, the ultrasonic sensor was activated by some background noises and appears to be incapable of more than a moderate degree of success in distinguishing pets. The E-field sensor

is susceptible to some pets, although considerable discrimination was achieved. It is also probably susceptible to activation by lightning, although it was not tested for that. Wide field-of-view passive infrared systems with commercially used spectral filters are susceptible to moving drapes, pets, moving shadows due to sunlight or other illumination, and to other heat sources. Wide field-of-view active infrared systems were not investigated, but they can be expected to respond to drapes, pets, and other movements within the field of view.

Consequently, it appears that the best opportunity for obtaining an acceptably low false alarm rate lies with those systems that provide a narrow field of view and thus obtain volumetric coverage via several narrow "beams" whose cross section is of the order of a few inches to a foot. This is because most common sources of false alarms can then be excluded from the field of view by proper installation. Since it is impractical to provide this degree of spatial discrimination with either the ultrasonic or E-field sensors, the infrared sensors, both active and passive, are the best prospects for future development.

Narrow field-of-view passive and active infrared sensors exhibited the expected immunity to false alarms from sources outside of the field of view. The passive sensor was somewhat susceptible to background variation, such as moving shadows, within the field of view because it must have substantial low frequency response in order to detect a slow-moving intruder. The active sensor provides an additional degree of freedom in that the illumination can be modulated at a relatively high frequency and the detection performed at that frequency. This provides a means of rejecting low frequency perturbations of the background. In practical terms, the active system can be installed with fewer restrictions on where it "looks." The passive system has fewer parts and consumes less power, making it potentially lower in cost and simpler to install.

B. Performance and Reliability Evaluation of a Passive Infrared Intruder Sensor

The following description is a summary of an Aerospace report³ prepared for the Law Enforcement Assistance Administration. The report documents a series of performance and evaluation tests conducted by the Optical Systems Department of Aerospace on the Rossin passive infrared intruder system, provides an assessment of the reliability of the detector used in the sensor, and recommends specific efforts to improve sensor performance.

1. Tests and results.

a. Functional performance. Two Rossin sensors were tested under conditions simulating a home, or apartment, environment. Output relays were attached to the inputs of a dual channel recorder to document the tests.

Positive detection occurred for both sensors at ranges of 2, 4, 6, 8, 10, 12, and 14 meters for a man walking across the field of view at about 0.7 meter per second; for a man walking quickly through the field of view, positive detection occurred in both sensors at ranges of 2, 8, and 14 meters. When a man crossed the beam from a running start, both sensors responded at a range of 4 meters, but neither responded reliably at a range of 2 meters: "missed target" sometimes occurred.

b. Household appliance electromagnetic interference. In these tests, the sensor was placed near an appliance that was activated through several operating cycles. Various appliances were used: television sets, a vacuum cleaner, an electric shaver, an electric toaster, an 8000 Btu 220-volt air conditioner, a vaporizer, a dishwasher, a clothes washer and dryer, and a sewing machine.

Operation of the sensor alarm relay applied power to a light-emitting diode that could be observed by test personnel. A person then walked through

the beam while the appliance was operating, testing for both false alarms (relay closure when the beam had not been crossed) and missed signals (failure of relay to close when target was in beam). Neither false alarms nor missed signals occurred during the tests.

c. False alarms from visible and infrared environment. Tests were made on the movement of shadows across a sunlit surface in the field of view. This simulated such conditions as a wall illuminated by the sun, or tree shadows, or clouds interrupting the sunbeam. The Rossin sensor responded to the moving shadow, generating a false alarm.

d. Sonic exposure. The Rossin sensor uses polyvinylidene fluoride pyroelectric material in the pyroelectric detector pair; this material produces an output voltage when stressed mechanically and is potentially subject to microphonics. Tests were made with a variable frequency sine wave, amplified and converted to sound waves. The function generator was swept from 1 to 100,000 Hz in five segments. Frequency response of the audio amplifier and the speakers limited the system output to a band from a few hertz to about 20,000 Hz. No false alarms resulted. Several sonic blasts of about 1-second duration, at intervals of 3 seconds, were made at frequencies of from 30 to 12,800 Hz without generating false alarms.

e. Temperature exposure. One sensor was exposed to high temperature (130°F and 140°F) for periods from 4 to 19 hours; another was exposed to a low temperature (0°F) for 10 hours. Response thereafter was satisfactory, and no apparent degradation in performance resulted.

f. Electromagnetic compatibility with simulated radio unit. A sensor transmitter was simulated, using a loop antenna and a laboratory radio frequency generator. The generator was operated at frequencies of 500 kHz and 1.7 MHz at 0.1-watt nominal power output, in continuous wave and in 1-second bursts. No false alarms resulted.

g. Electromagnetic interference from commercial radio station and high-voltage powerlines. The sensor was operated at close range (500 to 1000 feet) to the transmitting antennas of a radio station with a power output of 50,000 watts. Two locations were used: one on line with the two towers; the other on the perpendicular bisector of that line. At each location, the sensors were tested in two orientations: one facing the towers, the other normal to the first. No false alarms or missed signals resulted.

Tests were made close (100 feet) to high-power voltage lines and at a similar distance from a power transformer complex. In neither test were there false alarms or missed signals.

h. Altitude exposure. Both medium-high (6500 feet above sea level) and low (280 feet below sea level)-altitude tests were made without false alarms or missed signals resulting.

2. Detector reliability assessment. The reliability evaluation mainly concerned the life of the polyvinylidene fluoride pyroelectric detectors. Detectors of this material are a recent development, and life data are limited. Obtaining life test data in the conventional way involves tests of long duration with a large sample population, both beyond the schedule and costs of the current program. As a result, reliability assessment at this point must be an engineering judgment based on current test results, the opinions of Government and industrial experts in the field, and existing technical literature. Two major contributions to this assessment were made by Mr. D. F. Stanfill of A. D. Little, and Dr. Gordon Day at the National Bureau of Standards.

Mr. Stanfill brought out the following comments:

- A.D. Little has been making polyvinylidene fluoride detectors for about a year and has not observed any appreciable decrease in performance with age.
- The uniformity of response is about 1 percent across a 1-cm-diameter detector.

- No degradation should be experienced at temperatures below about 70°C.

Dr. Day brought out the following comments:

- Output of two out of three such detectors dropped about 1 part in 10^4 per day during a 100-day test. Output of the third detector remained constant.
- Detectors exposed to temperatures of 140°F experienced a one-time-only drop of 10 percent in output, with no further drop in subsequent high-temperature cycling.
- Polyvinylidene fluoride detectors have been operated at temperatures as low as 77 K, and low-temperature exposure in the home environment would not be expected to harm the sensor.

On the basis of this information, the engineering judgment is that polyvinylidene fluoride detectors can be expected to give satisfactory life service in burglar alarm systems.

3. Conclusions and recommendations. The Rossin passive infrared intruder sensor is virtually immune to false alarms and missed targets due to thermal, sonic, and electromagnetic environments.

The Rossin sensor is effective over a range of 50-plus feet, for an appreciable range of target angular velocities.

The sensor is subject to missed alarms when an intruder runs through the field of view at close range. Subsequent to the tests, the Rossin Corporation modified the circuitry to improve performance. One result has been an improvement in the capability of the sensor to detect more rapidly moving objects; this improvement has been demonstrated but not tested to measure the new limits of performance.

Tests showed that the sensor is subject to false alarms caused by moving shadows on sunlit surfaces within its field of view. Again, events since the tests have shown that a thin sheet of black polyethylene can be used as a

filter to reduce or eliminate false alarms without seriously reducing the operating range. Furthermore, the Rossin Corporation has indicated that increasing the thickness of the magnesium oxide coating on the mirror in the device would be expected to reduce the false alarms from shadow-sunlight phenomena.

It was recommended that the Rossin sensor be used as is, or with minor modification, as a component in testing the full burglar alarm system.

It was recommended that the use of two or more beams be implemented, using mirrors sharing the sensor aperture, to determine the response of the sensor to rapidly moving targets.

Recommendations on circuit design modifications and the reduction or elimination of susceptibility to false alarms resulting from the sunlight-shadow effect were made; these have been accomplished in part by more recent events but remain subject to test and measurement.

C. Rossin Corporation Thermal Intruder Sensor

The Rossin device responds to thermal radiation changes it sees when an intruder moves across the area viewed by the sensor. This actuates a relay which may be used to sound an alarm. The intruder can be either warmer or cooler than the ambient environment.

The sensor (refer to Fig. 36) is a passive infrared sensing device. It consists of an optical system, a pair of pyroelectric detectors, and simple electronic circuitry for actuating an alarm relay. A schematic diagram of the unit is shown in Figure 39.

The sensor has a field of view about 2 feet in diameter at a range of 50 feet, a distance less than the maximum effective range, and has an appreciable range of target angular velocities. The pyroelectric detectors are sensitive to a broad range of visible and infrared wavelengths; they are connected to a 10^{12} -ohm load resistor and the electronic circuitry to amplify

Figure 39. Rossin Thermal Intruder Sensor, Schematic Diagram

and process the output of the detectors to actuate the alarm relay. The logic relay latches on for 1 second when an intruder moves through the field of view and then is not usable for an additional 20 seconds.

Use of the Rossin sensor is recommended for pilot testing of the integrated burglar alarm system. Testing has shown it to be almost immune to false alarms and missed targets. Its reliability, although not fully assessed in life tests, is considered satisfactory based on the available data and engineering judgment. Three vulnerabilities encountered in the tests conducted (missed targets on short-range, fast-moving intruders, and false alarms resulting from sunlight-shadow effects) have resulted in recent modifications and proposed solutions to reduce or eliminate the undesired characteristics.

1. The modified Rossin device. The modified Rossin device is the result of follow-on developments to eliminate the initial deficiencies. It has satisfactorily completed limited testing.

Several filter materials were tested to prevent false alarms from moving shadows. Thin (0.0006-inch) black polyethylene sheet filters virtually eliminated this problem, with a reduction in operating range to about 35 feet, still sufficient, however, for large residential rooms and small business applications.

A two-beam modification was invented by J. J. Redmann, The Aerospace Corporation, to improve detection of short-range and fast-moving targets. This consisted of an aluminum plate pivoted in front of the optical aperture and held at an adjusted angle by a clamp screw. The aluminum plate serves as a mirror for the infrared wavelengths. This permits the sensor to view straight ahead with half its optical aperture, and to a side with the other half (see Fig. 40). The side-viewing feature is adjustable, as previously noted, to obtain an optimum angle for the site of the installed sensor. The modification, using a stamped aluminum part and a clamp, is

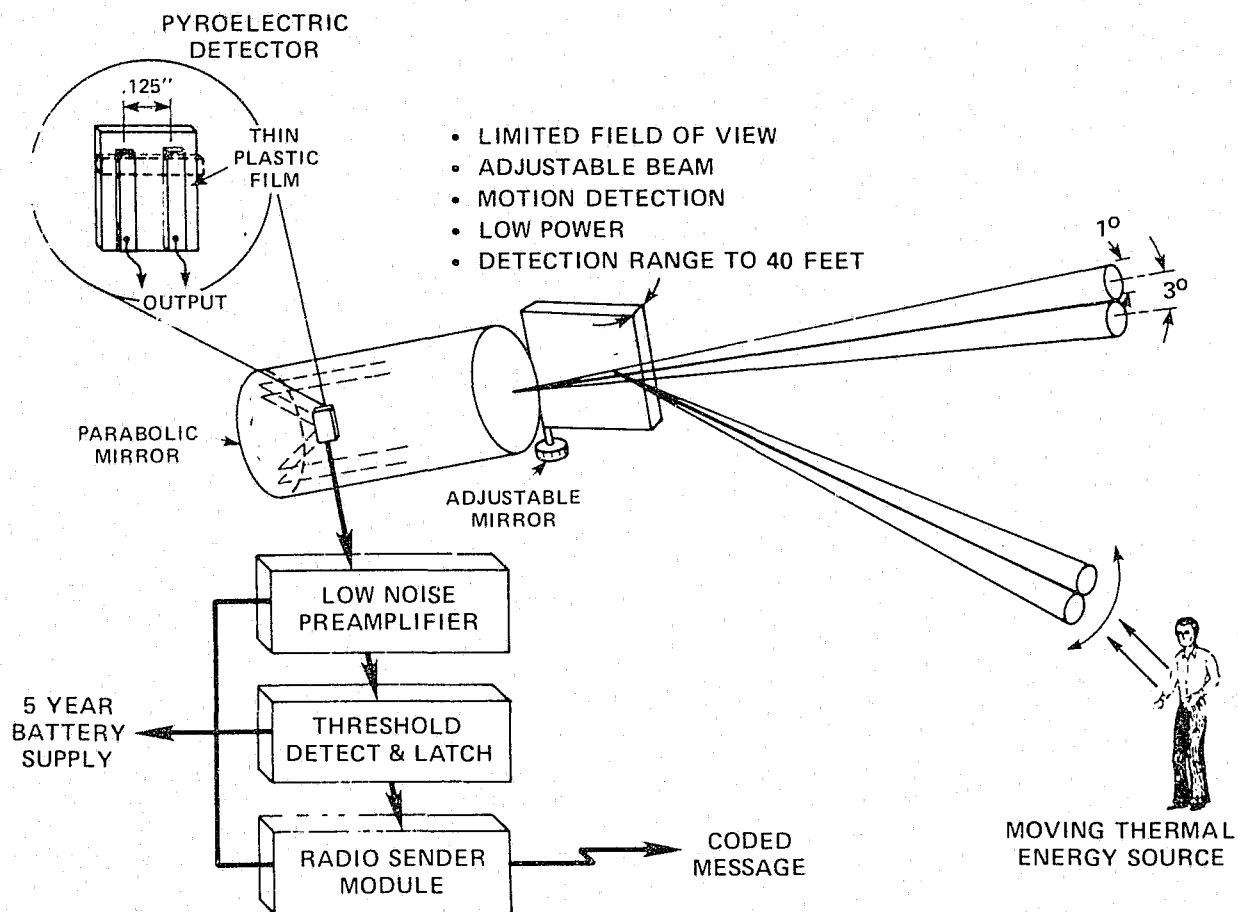


Figure 40. Improved Thermal Intrusion Sensor with Two-Beam Mirror

inexpensive. It reduces the effective operating range by about 30 percent, which is considered an adequate tradeoff for improved acquisition of close and fast-moving targets.

Concurrent with these developments, the Rossin Corporation improved the electronic circuitry of the original models to decrease the response time for fast-moving targets.

Figure 14, page 48, shows the improved device in an operational mode.



CHAPTER V. FUTURE DEVELOPMENTS

A. Improved Adaptive Alarm System

The improved adaptive alarm system was defined and the hardware was being developed when the program was discontinued. This improved system concept indicates that the full application of a burglary alarm system demands exterior communication with a central station for fire, police, and emergency services. The component described in this section is a control unit designed to provide external communication as well as internal functions on the protected premises.

1. Design goals. Several goals guide the design of this burglar alarm system (Fig. 41).

a. Flexibility. The system is intended to be extremely flexible to serve both the agencies providing burglary and related alarm services and the users who are subscribing to these services. The unit is designed as a component with no particular system manufacturer in mind. The component is applicable to small and large system designs and to a variety of marketing approaches. The system is portable from one premises to another.

b. Low cost. The system is designed for the lower-priced market. It is intended for use by moderate-income homeowners and proprietors of businesses in small- to medium-size premises. This is achieved by using the radio connection from intrusion detectors and other sensors to the control unit, which eliminates the need for on-premises wiring.

c. Reliability. The system must reduce false alarms by testing and verifying possible intrusion signals before initiating a call to the service provider. The service user is given warning to permit him to terminate a false alarm sequence prior to its being transmitted to the service provider's central station.

d. Marketability. The system must be simple to use and inexpensive to install. It will be adapted to a variety of sensors and auxiliary functions for wide application. It will be usable with sensors from many kinds of devices. It will generate telephone alarm messages for transmission to remote computers and coded rhythmic "tones" for audible alerting signals.

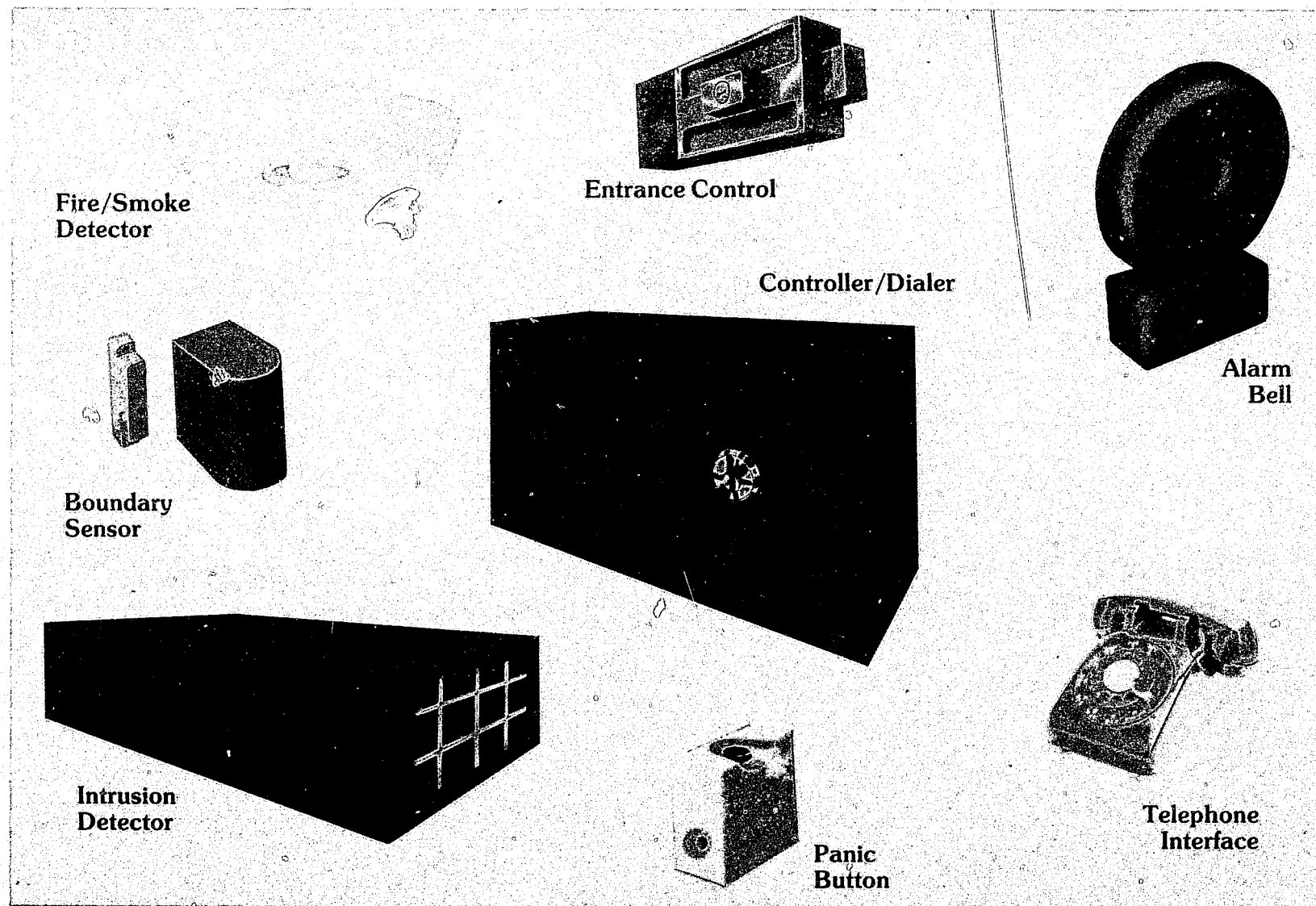


Figure 41. Total System Package for Mod II Microprocessor

2. Operational concept. Each premises control unit will be used at a single location. A unit will serve up to 32 sensing devices which communicate to it by means of miniature radio-sending modules. The radio senders will be located at door locks, windows, doors, floor switchmats, motion sensors, infrared detectors, thermostats, personal button-controlled units, and other desired control points.

The control unit incorporates a radio receiver to detect signals from these senders and to shift them into a microcomputer. The microcomputer goes through a prescribed sequence to interpret the signal. Signals from the locks arm and disarm the control unit. Signals from intrusion sensors are ignored when the system is disarmed and initiate alarm sequences when it is alarmed. Fire, tamper, radio jamming, and personal emergency (panic) signals always initiate alarms.

The alarm sequence produces first an easily recognized warning tone, during which time a person possessing the correct key can disarm the system and inhibit further alarm. If the sequence is allowed to continue, it sounds a burglar or fire alarm bell on the premises and initiates a telephone call to one of a set of telephone numbers. The alarm sequence then transmits a computer interpretable message identifying the premises and indicating the status of every connected sensor. The central station must be supported by a computer compatible with the system and must have provision to decode and display the transmitted message.

When a subscriber first installs the premises control unit, provision must be made to connect it to his telephone service, either through a conventional telephone company jack, or through a more sophisticated dial director; control signals are provided for both kinds of installation. Then, using a key to gain access, the subscriber goes through a "memorize" sequence that first involves dialing the central station and coordinating with an operator there.

This operator will cause the central station computer to transmit, automatically via the phone line, a tailored set of telephone numbers, identification sequences, and operational delays to the premises unit. This information will be retained indefinitely, but may be revised at any time by repeating the process.

The user then sorts his radio transmitters into classes by function and identifies each transmitter with a unique channel number to be used by the control unit. Using controls on the central unit, he then cycles successively through the 32 available channels and activates the respective radio transmitter when its matching channel number is displayed. This procedure causes the central unit to memorize the unique radio signal from each transmitter and to associate it with the selected channel number. Each radio transmitter transmits its own unique 15-binary-digit code. There are 32,768 different combinations. The radio range is useful up to 40-50 feet.

Key-activated transmitters will cause the system to be armed or disarmed. Typically the key will be used to lock a last door of exit from the outside, or a final door of security from the inside. The system reacts differently when armed from the outside than when it is armed from the inside. At the time the system is armed, the central unit will briefly indicate sensor units that are not secure, such as open windows and unlocked doors. If any such condition is not corrected and is followed by a rearming of the system, the unsecured sensors will be ignored for the purposes of detecting intrusions until some subsequent rearming sequence is executed.

a. Operating modes. There are six system-operating modes (see Table 5).

- Disarmed — In this mode, the alarm system monitors all sensors and updates their status, but does not recognize an alarm condition for intrusion sensors. Fire sensors, personal emergency signals, and tampering still generate an alarm.

Table 5. System Operating Modes

Function	Disarmed	Armed inside	Armed outside	Test mode	Memorize data	Memorize sensor ID
Sensors	Internal: monitored Boundary: monitored	Internal: monitored Boundary: armed	Internal: armed Boundary: armed			
Alarm	Fire and emergency only	Fire Emergency Boundary	Fire Emergency Internal Boundary	All functions monitored and reported on command	For setting telephone numbers, registration data, alarm delay intervals	For setting channel ID numbers of sensors
Other functions	Operational	Operational	Operational			

- Armed from inside — In this mode, the alarm system will ignore internal sensors (such as floormats and motion detectors) though their status will be monitored. Boundary sensors (such as doors and windows) will generate an alarm condition if activated. Fire and emergency sensors are active.
- Armed from outside — All sensors in the alarm system are active in this mode and are continually monitored for intrusion conditions. Any activation of a boundary sensor, fire alarm, or emergency button will generate an alarm condition. Any two signals from internal sensors must be detected within 5 minutes, however, in order to generate an alarm.
- Test modes — The microprocessor recognizes test conditions although they are not separate system modes. The actual system may be in an armed or disarmed mode and will function as if it is in a nontest condition. Any transmitted alarm message to the central station will indicate that a test is being performed. The local test condition is the same, except that telephone calls are not initiated.
- Memorize data from base station — The microcomputer can record telephone numbers, registration identification data, and alarm-delay intervals from a message transmitted from the base station. In this mode, the alarm system ignores all the sensors.
- Memorize sensor identification signals — In this mode, used when installing or changing sensors, the transmitted sensor signal is associated with a unique channel number and recorded in the microcomputer memory.

3. Operational controls. User controls will depend on the manufacturer of production models. The capability of the control unit, however, allows the following control features.

a. User external controls. The control unit housing will provide for a key-controlled switch, a pushbutton, and an eight-segment (seven-segment numeral and decimal point) display. The key will also unlock the housing for service. The switch may have the following four positions (see Table 6).

- Normal
- Full test
- Local test
- Memorize

The pushbutton may act as a fire alarm reset button in the normal mode. When the key switch position is set to "Memorize," however, the pushbutton may be used to select channel numbers for the sensors and assign sensor identification signals for memorization by the controller.

4. Display. The seven-segment hexadecimal numeral display will allow the showing of 16 characters (Fig. 42). The decimal point may be used with the characters to indicate the 32 channels available for sensor identification (16 without the decimal point, 16 with the decimal).

a. Pilot display. The characters will flash periodically during periods of normal operation to indicate the following:

- Armed from outside
- Armed from inside
- Disarmed

b. Telephone dialed-digit display. During telephone dialing, the digit momentarily being dialed is displayed.

c. Active channel display. When a sensor activates the control unit on its respective channel, the channel number is displayed for a short interval.

Table 6. Key Switch Positions

	Normal — usual switch position	Full Test	Local Test	Memorize
Status of systems	All in function	All in function	Telephone connections inhibited	
Status of alarm	Ready	Alarm bell sounds on test	Alarm bell sounds on test	Inhibited
Input to controller	Status: Disarmed Armed inside Armed outside	Notified of test condition	Notified of test condition	Notified of memorize condition Telephone number on command Sensor identification number on command
Input to telephone stations	Alarm calls Data messages	Notified of test condition	None	

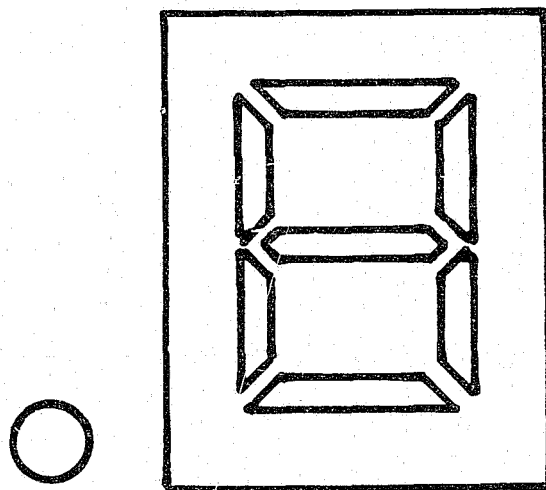


Figure 42. Seven-Segment Hexadecimal Numeral Display

d. Associated channel number display. During the "memorize sensor identification signals" mode, the channel number with which the sensor will be associated is displayed until changed. The 32 channels are stepped through cyclically, advancing one channel number each time the button on the housing is depressed.

e. Unsecured boundary channel display. The number of each channel recorded in the computer as having last reported an unsecure condition will be displayed at the time of arming.

5. Internal controls. Internal controls are provided for maintenance, installation, and protection.

a. Tamper switch. If the control unit housing is opened without using the key, a "tamper" switch will be activated. The unit will forthwith initiate a telephone call with a message indicating the tampering.

b. System reset (power start). A switch is provided for maintenance use to restore correct operation after a power outage.

6. Alerting/warning signal tone. An audible tone generator, which emits an audible buzzing squeal, is incorporated in the housing. When pulsed briefly, it emits a "beep." When it is sounded in a sustained manner, it is a somewhat annoying, easy-to-hear signal.

a. Memorize data from base station. Each time the control unit records an identification signal, it emits a beep.

b. Burglar alarm warning. Prior to sounding the alarm bell for burglary, the audible tone is sounded steadily for about 20 seconds (variable delay).

c. Fire alarm warning. Prior to sounding the alarm bell for a fire, the audible tone is sounded intermittently for about 20 seconds (variable delay).

d. Unsecured boundary channel. If, at the time of arming, a boundary sensor has previously reported an unsecure condition, the control unit will emit a series of beeps.

7. Wiring connections. The control unit has terminals or jacks to provide for wired connections to external devices.

a. Power. The control unit will have a standard power cord that must be plugged into a standard 115-volt 60-Hz household outlet. A battery will sustain operation during short periods of power outage.

b. Telephone. Two telephone connectors are provided. The first presents a signal during periods when telephone service is requested to make outgoing calls. The signal is available to operate call director-type equipment. The second telephone connector provides dial pulses, asynchronous frequency-shift-keying coded data groups for computer-to-computer data transmission, and coded sequences of beeps for telephone alerting signals. The second signal is intended for direct interface with the Bell System network facilities. Provision is also made to output a dialing digit to a dual-tone multifrequency generator to simulate touch-tone dialing.

c. Alarm bell. A connector is provided to control the sounding of an alarm bell. The signal will initiate a programmed delay of approximately 20 seconds in the alarm unit itself, followed by the ringing of the bell for a minimum interval (such as 15 minutes). Once initiated, this sequence will ensue even though the control cable is severed. The control signal will be pulsed to control the bell's ringing so that a fire alarm will be distinguishable from a burglar alarm.

8. Electric locking-door strike. A connector is provided to control the automatic locking of doors, using an electrically controlled strike in the door frames. A signal is present when the system is armed from the outside.

9. Auxiliary unit controls. Four connectors are provided to control signals to four local auxiliary devices. A signal is present during those times when the respective auxiliary device sensor sender has transmitted a set signal, until such time as it has transmitted a reset signal.

10. Radio receiver input. The change of status of all sensors, locks, and auxiliary devices is relayed to the central unit by a near-field radio transmitter at the time that the change is detected. The radio receiver is active unless the premises central unit is in the mode to memorize data from the central station. The radio receiver will be housed in the same enclosure as the premises control unit and will not be identifiable by the user as a separate component.

There is no signal back to the transmitter verifying that the status change signal has been correctly received. The radio receiver clocks in 16 binary digits of message to a storage shift register and then sets a flag to notify the microcomputer that the message is available for processing. The microcomputer will provide clock pulses to the shift register to read in the data, and, upon completion of read-in, it will reset the message-available flag.

The radio receiver will detect the sustained presence of a received signal that bears no data. If the signal persists sufficiently long, it will set a flag that indicates to the control unit that radio frequency interference is present.

B. Central Station Design

The central station (police or private security) should operate as the central controller for a group of premises protected by compatible burglar alarm systems. It should provide the timing and control required to transfer the data from adaptive alarm system control units to operating personnel in the security station.

1. Performance requirements. The central station should satisfy a number of performance requirements.

a. Capacity.

- User identification — The central station must be capable of identifying a minimum of 1000 adaptive alarm system control units, representing a minimum of 1000 users.
- Detector identification — The central station must be capable of identifying up to 32,000 alarm sensor units.
- Multiple alarms — The central station must be capable of simultaneously accepting alarm data from three different adaptive alarm system control units.

b. Data transmission.

- Link integrity — Once activated by an adaptive alarm system control unit, the central station will maintain the data link between the control unit and the central station until released by the central station operator.
- Two-way communication between the central station and the adaptive alarm system control unit will be provided. The data rate and format must be compatible with the microprocessor requirements.

c. Data processing.

- Alarm type — The data received from an adaptive alarm system control unit will be processed and the alarm identified as one of the following types of alarms: self-test, intrusion, fire, panic, or radio frequency interference.
- Operator updating — The central station should accept changes in user, or sensor, identification and location data changes when entered by the operator.

- Alarm sensor status — Changes in the status of an alarm sensor that occur during an alarm condition will be recognized and displayed by the central station.
- d. Data presentation.
- Video — A video presentation of the alarm data, containing (as a minimum) the information presented in Figure 43, should be made automatically to the central station operator. The system must be capable of displaying the status of at least 32 detectors. For each user control unit alarm, only the detectors actually installed and their status should be displayed. Activated sensors must be uniquely displayed (e.g., flashing). The existence of a second and third alarm should be indicated but should not over-write the video display, and the data should be cued for use on the video display.
 - Hard copy — A hard copy printout of the data presented to the central station operator will be made. Additionally, changes made by keyboard entry will be printed.
 - Multiple alarms — The existence of multiple alarms must be identified to the central station operator in such a way as to establish a handling priority for the operator.
 - Temporary storage — In the event of multiple alarms, the central station will be capable of placing sufficient alarm data in temporary storage for later retrieval and processing. The transfer of alarm data from the video terminal display to temporary storage must be done only on command from the central station operator.



e. Data management. The central station should maintain a record of all alarm data for easy retrieval of data on individual alarms, alarms by categories, and alarms within a specific time interval.

2. Hardware. The central station should use commercial hardware (microprocessor/minicomputer) and off-the-shelf peripheral equipment as required. The maximum envelope of the central station hardware, excluding the hard copy printer, will be 24 inches wide, 36 inches deep, and 36 inches high.

3. Software. The optional software in conjunction with the hardware will, as a minimum, support the following functions:

- Controlling the transmission of data from each control unit to the central station
- Accepting data from each control unit in the form of alarm data or status verification information
- Performing internal table look-up, data comparison, and assignment of priorities
- Initiating output interface commands
- Monitoring control of all system functions
- Adding or deleting user and control unit identification or location data
- Exercising data management, permitting the periodic retrieval of alarm and user data

Computer programs in support of the operational software must not destroy or alter the data base if a fault occurs. Furthermore, the event of a channel or link failure should not inhibit the software from responding to an alarm received from another control unit. In the event of power interruption, the software should be automatically loaded so that the system can reach operational status automatically.

a. Software language. Programming of the central station computer software should be accomplished using a high-order language (e.g., Fortran). Machine peculiar or special purpose languages shall not be used.

NOTES

1. "Survey and System Concepts for a Low Cost Burglary Alarm System for Residences and Small Businesses," Report No. ATR-74(7904)-1, Reissue A, El Segundo, Calif., The Aerospace Corporation (August 1976).
2. R. F. Cannata, N. A. Mas, J. J. Redmann, J. A. Rowe, and E. N. Skomal, "Investigation of Burglary Alarm Sensors," Report No. ATR-76(7904)-2, El Segundo, Calif., The Aerospace Corporation (July 1976).
3. J. J. Redmann, "Performance and Reliability Evaluation of a Passive Infrared Intruder Sensor," Report No. ATR-76(7904)-1, El Segundo, Calif., The Aerospace Corporation (March 1976).
4. "Experimental Measurement of Path Noise in Ultra-Narrowband Radio Systems," El Segundo, Calif., The Aerospace Corporation (June 1977).

END